

USAISEC

*US Army Information Systems Engineering Command
Fort Huachuca, AZ 85613-5300*

4

AD-A220 179

U.S. ARMY INSTITUTE FOR RESEARCH
IN MANAGEMENT INFORMATION,
COMMUNICATIONS, AND COMPUTER SCIENCES
(AIRMICS)

Message Handling in the Post-2000 Era:

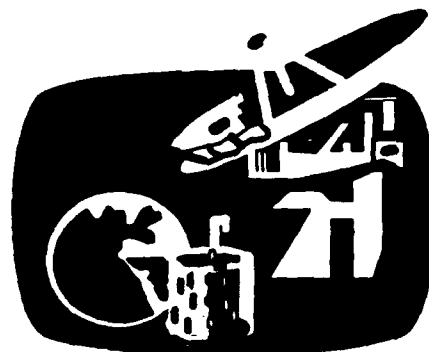
(ASQB-GC-90-003)

November, 1989

NOV 1989
E
CP



115 O'Keefe Bldg
Georgia Institute of Technology
Atlanta, GA 30332-0800



90 00 00 100

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704--188
Exp. Date: Jun 30, 1986

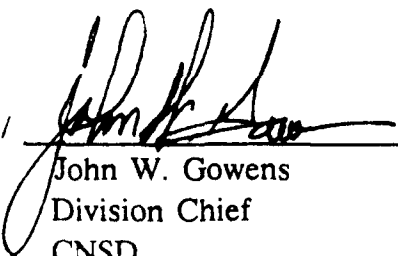
1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED			1b. RESTRICTIVE MARKINGS NATO														
2a. SECURITY CLASSIFICATION AUTHORITY N/A			3. DISTRIBUTION / AVAILABILITY OF REPORT Unclassified/Unlimited														
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE N/A																	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) N/A			5. MONITORING ORGANIZATION REPORT NUMBER(S) ASQB-GC-90-003														
6a. NAME OF PERFORMING ORGANIZATION Georgia Institute of Tech. Electrical Engineering		6b. OFFICE SYMBOL (if applicable) N/A	7a. NAME OF MONITORING ORGANIZATION AIRMICS														
6c. ADDRESS (City, State, and ZIP Code) Atlanta, GA 30332-0250			7b. ADDRESS (City, State, and Zip Code) 115 O'Keefe Bldg., Georgia Institute of Technology Atlanta, GA 30332-0800														
8a. NAME OF FUNDING/SPONSORING ORGANIZATION NATO/U.S. Army Signal Corp.		8b. OFFICE SYMBOL (if applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER														
8c. ADDRESS (City, State, and ZIP Code) U.S. Army Signal Center Fort Gordon, GA 30905-5090			10. SOURCE OF FUNDING NUMBERS														
			PROGRAM ELEMENT NO. 612T83	PROJECT NO. DY10-03-01	TASK NO. 08												
11. TITLE (Include Security Classification) Message Handling in the Post-2000 Era: (UNCLASSIFIED)																	
12. PERSONAL AUTHOR(S) Browning, Douglas W., Wicker, Stephen B.																	
13a. TYPE OF REPORT Final		13b. TIME COVERED FROM 2/15/89 TO 11/30/89		14. DATE OF REPORT (Year, Month, Day) 1989 November 17													
15. PAGE COUNT 91																	
16. SUPPLEMENTARY NOTATION																	
17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)														
<table border="1"><thead><tr><th>FIELD</th><th>GROUP</th><th>SUB-GROUP</th></tr></thead><tbody><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></tbody></table>			FIELD	GROUP	SUB-GROUP										communications Communications, Networks, Post-2000		
FIELD	GROUP	SUB-GROUP															
19. ABSTRACT (Continue on reverse if necessary and identify by block number) Communication architecture for message handling in the very far-term heavy tactical environment are considered. The projected limitations of technology, a taxonomy of possible architectures, and projected requirements are presented. Based on this information, the suitability of architectural options is analyzed, and an architecture is proposed for post-2000 mobile and nonmobile tactical communications. The implications for standards are discussed.																	
20. DISTRIBUTION / AVAILABILITY OF ABSTRACT <input checked="" type="checkbox"/> UNCLASSIFIED / UNLIMITED <input type="checkbox"/> SAME AS RPT. <input type="checkbox"/> DTIC USERS			21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED														
22a. NAME OF RESPONSIBLE INDIVIDUAL WINFRED Y. FONG			22b. TELEPHONE (Include Area Code) (404) 894-3136		22c. OFFICE SYMBOL ASQB-GC												


This work is done under contract DAKF11-86-D-0015 for the United States Army Institute for Research in Management Information, Communications, and Computer Sciences (AIRMICS), the RDTE organization of the United States Army Information Systems Engineering Command (USAISEC). This report is not to be construed as an official Army position, unless so designated by other authorized documents. The material included herein is approved for public release, distribution unlimited. Not protected by copyright laws.

Accession For	
NTIS GRA&I	<input checked="checked" type="checkbox"/>
DTIC TAB	<input checked="checked" type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By _____	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

THIS REPORT HAS BEEN REVIEWED AND IS APPROVED



s/ 
John W. Gowens
Division Chief
CNSD

s/ 
John R. Mitchell
Director
AIRMICS

CONTENTS

1. Identification of Options	1
1.1. Introduction.....	1
1.1.1. On the Past and Future History of Communication.....	1
1.1.2. Fundamental Architectural Alternatives.....	3
1.2. Media Options	3
1.2.1. Propagation through Atmospheric/Free-Space Channels.....	4
1.2.1.1. Long-Distance Atmospheric Transmission.....	5
1.2.1.2. Line-of-Sight Transmission.....	7
1.2.1.3. Sub-Orbital Platforms.....	8
1.2.1.4. LEO Satellite.....	9
1.2.1.5. Geosynchronous Satellite.....	9
1.2.2. Propagation through Confined Channels.....	9
1.2.2.1. Wire.....	11
1.2.2.2. Optical Fiber.....	11
1.2.2.3. Recording Media.....	11
1.2.3. Multi-Media Switching.....	11
1.3. Data Encryption Options	12
1.3.1. Private Key Encryption Techniques.....	15
1.3.2. Public Key Encryption Techniques.....	16
1.3.3. Combined Public/Private Key Systems.....	17
1.4. Communication Subnet Architectural Alternatives.....	18
1.4.1. Fundamental Choices.....	18
1.4.2. Single-Hop Networks.....	20
1.4.2.1. Single point-to-point links.....	20
1.4.2.2. Broadcast through confined channels.....	20
1.4.2.3. Broadcast on Atmospheric Channels.....	23
1.4.2.4. Single-Repeater Systems.....	23
1.4.2.4.1. Geosynchronous Satellite Access.....	24

1.4.2.4.2. Other Single-Repeater Systems.....	26
1.4.2.5. Directional Propagation on confined channels.....	26
1.4.2.6. Rings.....	27
1.4.2.7. Double Rings.....	28
1.4.3. Multi-Hop Networks.....	29
1.4.3.1. Topologies.....	29
1.4.3.2. Circuit-Switching, Packet-Switching, and Alternatives.....	29
1.4.3.3. Routing.....	30
1.4.3.4. Flow Control.....	30
1.4.3.5. Point-to-Point Channels.....	31
1.4.3.5.1. Store-and-Forward Mesh.....	31
1.4.3.5.2. Interconnection Networks.....	32
1.4.3.5.3. Cellular Radio.....	33
1.4.3.6. Broadcast Channels.....	34
1.4.3.6.1. Partially Overlapping Broadcasts.....	34
1.4.3.6.1.1. Connectivity.....	34
1.4.3.6.1.2. Channel Access.....	36
1.4.3.6.1.3. Link management.....	37
1.4.3.6.1.4. Routing.....	38
1.4.3.6.1.5. Flow Control.....	39
1.4.3.6.1.6. Deployment and Maintenance.....	39
1.4.3.6.2. Non-Overlapping Broadcasts.....	40
1.4.3.7. Hybrid Architectures.....	41
1.5. Internetworking Options.....	41
1.5.1. Gateways.....	41
1.5.1.1. Gateways for Packet Radio Networks.....	41
1.6. Higher Layer Options.....	42
2. Requirements and the Suitability of Options for Non-Mobile Subscribers.....	43
2.1. Requirements.....	43

2.1.1.	NATO Requirements	43
2.1.2.	US Army Requirements	44
2.1.3.	US Air Force Requirements	45
2.1.3.1.	Current Air Force Communication Outlook.....	45
2.1.3.1.2.	The Air Force's Tactical C2 Environment.....	46
2.1.3.1.3.	The Air Force's View of the Communications Environment.....	48
2.1.4.	Navy Requirements	50
2.1.5.	Defense Communication Agency Requirements.....	50
2.2.	Suitability of Options	52
2.2.1.	Long-Haul Communication.....	52
2.2.1.1.	Physical Channel Options.....	53
2.2.1.2.	Networking Options.....	54
2.2.1.2.1.	A Single-Repeater Broadcast System.....	54
2.2.1.2.2.	One Point-to-Point Mesh.....	54
2.2.1.2.3.	Several Point-to-Point Meshes	55
2.2.1.3.	Higher-Level Options.....	55
2.2.2.	Base Level Systems.....	55
2.2.2.1.	Physical Channel Options.....	55
2.2.2.2.	Networking Options.....	56
2.2.2.2.1.	Individual point-to-point connections.....	56
2.2.2.2.2.	General Mesh Architectures	56
2.2.2.2.3.	Single-Hop Directional Propagation Systems.....	57
2.2.2.2.4.	Rings.....	57
2.2.2.2.5.	Double Rings	58
2.2.2.2.6.	Interconnected LANs.....	58
2.2.2.2.7.	Constrained Meshes.....	59
2.2.2.3.	Internetworking with Long-Haul Communication Systems.....	59

2.2.3. Local Area Systems.....	59
2.2.3.1. Physical Channel Options.....	59
2.2.3.2. Networking Options.....	60
2.2.3.3. Internetworking with Base Level and Long-Haul Communication Systems.....	61
2.2.3.4. Higher-Level Options.....	61
3. Requirements and the Suitability of Options for Mobile Subscribers.....	62
3.1. Requirements.....	62
3.1.1. Air Force Requirements.....	62
3.1.2. Army Requirements.....	63
3.2. Suitability of Options.....	63
3.2.1. Long-Range Mobile Communication.....	64
3.2.2. Medium-Range Mobile Communication.....	65
3.2.2.1. Packet Radio Networks.....	66
3.2.2.2. Cellular Radio Networks.....	66
3.2.2.3. Hybrid Networks.....	67
3.2.3. Local Area Mobile Communications.....	67
3.2.4. Connection from Mobile Systems to a Long- Haul Non-Mobile Network.....	68
3.2.4.1. Local Connection.....	69
3.2.4.2. Over-the-Horizon Radio.....	69
3.2.4.3. Satellite Channels.....	69
3.2.4.4. Commandeered Public Communication Channels.....	69
3.2.5. Connection from Local Area Mobile Systems to Medium-Range Mobile Systems.....	70
3.2.6. Communication to and from the Mobile Command Post.....	70
3.2.7. Communication within the Mobile Command Post.....	70
3.2.8. Aircraft Communication.....	72
3.2.8.1. Long-Range Communication.....	72
3.2.8.2. Communication within an Airborne Formation.....	72

4. Recommendation of a Message Switching Architecture for the Post 2000 Tactical Communications System.....	73
4.1. Non-Mobile Long-Haul Communications.....	74
4.2. Non-Mobile Base-Level Communications.....	74
4.3. Non-Mobile Local Area Communications.....	76
4.4. Ground-Based Mobile Medium-Range Communication.....	77
4.5. Ground-Based Mobile Local Area Communication.....	77
4.6. Communication for the Mobile Command Post.....	77
4.7. Airborne Communication.....	78
5. Standards for the Land Combat Zone.....	79
5.1. An Approach to Development of Standards for the Post-2000 Tactical Environment.....	79
5.2. Physical, Media Access, and Network Layer Standards.....	80
5.2.1. Non-Mobile Communication Standards.....	80
5.2.1.1. Non-Mobile Local Area Communications.....	80
5.2.1.2. Base-Level Communications.....	80
5.2.1.3. Non-Mobile Long-Haul Communications.....	80
5.2.1.4. Interfacing among Long-Haul Non-Mobile Networks.....	81
5.2.2. Mobile Communication Standards.....	81
5.3.1. Connection from Long-Haul Non-Mobile Networks to Medium-Range Mobile Networks.....	81
5.3.2. Medium-Range Mobile Networks.....	81
5.3.3. Interface from Medium-Range to Mobile Local Area Networks.....	82
5.3.4. Mobile Local Area Networks.....	82
5.3.5. Communications within a Mobile Command Post.....	82
5.3.6. Aircraft Communications.....	82
5.3. Higher-Layer Standards.....	83

1. Identification of Options

1.1. Introduction

1.1.1. On the Past and Future History of Communication

In a historical review of communication networks, beginning with the earliest telephone networks and even the telegraph systems that preceded them, there are three fundamental principles that stand out with amazing consistency¹:

- the most expensive component of a communication network is the media by which a signal is carried over a large distance
- communication network technology has been limited primarily by the ability to handle information at each switching point
- applications of larger, faster, and more efficient communication systems have always far surpassed the most far-sighted intentions of the developers².

The first principle dictates that any effective system design must include an efficient use of the expensive long distance media, but the second indicates that once the ability to handle a particular type and rate of traffic has been developed, the media to transmit the data has always been readily available.

Thus, the basic approach to network design in the past has been to first ask the question, "How well are we able to process the data?" and then to use communication channels at that rate.

These principles can be seen in recent history in such things as the only recent emergence of commercially available packet switching at T1 rates, and the push for integration of different data types on single networks to provide better sharing of the expensive channels and to simplify administration.

Although a projection a few decades into the future must be considered very approximate, there is no evidence that these principles will not hold for the foreseeable future. For example, optical fibers have already been developed that have essentially infinite capacity, but the photonic switching devices to handle and

switch data at very high rates are still in the earliest stages of development.

One possible exception is that ultimately the use of atmospheric propagation may be limited by the usable bandwidth of frequencies rather than switching technologies. The attenuation at high frequencies will impose strong restrictions on the use of frequencies in the upper range, so that bandwidth will continue to be an increasingly scarce resource.

There are certain elements of a communication system which can be expected to be present in any future architecture. A list of these include:

- a variety of data types with very different performance criteria: in fact, the current common characterization of interactive data, file transfer, voice, and video is expected to predominate, although other data types may be added
- a layered approach to system architecture design
- packets: some data, if not all, will be organized into units convenient for the communication system, and will be passed through the communication system as a unit
- acknowledgement structures: while it is possible that forward error correcting may be developed to the point that the reliance on acknowledgement systems will be greatly reduced, their advantages for assurance of reception are obvious and are likely to be maintained
- switching/routing devices: devices which switch and route data units
- a variety of standards that must be able to interact at some level

In addition, several basic trends can be expected which will influence the nature of future communication systems:

- the sophistication of data systems will increase, so that increasing computing effort will be placed on the task of providing user-friendly input and presentation of data in forms most easily used by human operators.
- the techniques available to be used in communication systems will become increasingly sophisticated. Many

current architectures have shortcomings that can be overcome by methods that are considered to be "too complicated." While the simplest method that overcomes a shortcoming will still be preferred, significant onboard processing should be significantly reduced as an architectural factor.

- data rate requirements will increase. This trend will be strongly countered by increasing sophistication in data compression techniques and wider distribution and storage of unvarying information, but the ever greater availability of electronic equipment and more data-hungry applications can be expected cause and increasing requirement to prevail.

1.1.2. Fundamental Architectural Alternatives

While the range of possible network architectures may be inexhaustible, there is a very limited set of reasonable architectural options. Where there is an infinite variety of channel configurations available, these can be easily classified into a few basic types. Encryption methods are also fairly uniform among various applications. Similarly since the wide variety of data types are likely to be using the same communication system and, except for differences in requirements on data rates, basically the same types of data will be transmitted on all types of communication system, the user needs at the transport layer and above should be similar irrespective of the network architecture. Therefore these issues are presented as individual sections.

Remaining are issues in the communication subnet architecture, as associated with the problems of Media Access, Logical Link Control, and Network Layer issues. Since these problems are highly dependent on the context within which they are applied, they are discussed in terms of a few basic architectural alternatives.

1.2. Media Options

All networks can be decomposed into a series of point-to-point communication links. The media selected for these links is an important consideration, for the various possibilities offer a wide range of positive and negative performance characteristics. The following pages discuss the media that will be the most useful in the design of message handling networks for the post-2000 tactical

environment. They are divided into two categories: atmospheric/free-space channels and confined channels (coaxial cable and the like). The performance criteria by which each medium is judged can be broken down into four general areas:

- deployment: the ease with which a communication system using the selected medium can be deployed on the battlefield.
- passive interception: the ability of the enemy to monitor channel traffic patterns and content
- active interception: the ability of the enemy to place spurious messages on the channel
- disruption: the ability of the enemy to reduce or eliminate the utility of the channel

1.2.1. Propagation through Atmospheric/Free-Space Channels

The earth's atmosphere and the free space above it provide an extremely convenient medium for communication. The communication channel is ubiquitous and thus presents no deployment problem in and of itself. This is an obvious benefit for mobile communication systems. To transmit or receive, one need only have an antenna and radio equipment capable of operation at the desired frequency. The radio transmitter superimposes an information signal onto a carrier and then propagates the result in the form of electromagnetic radiation. The amount of information that can be placed on the carrier is a function of carrier frequency. The carrier frequency also determines how far the signal will travel and the degree of susceptibility to enemy action. Carrier frequencies are usually grouped into the general ranges shown in Table 1.

Each range has its own unique qualities that make it useful for some applications, less so for others. Several general rules of thumb should be kept in mind. As carrier frequency increases, the following effects can be noted:

- carrier reflections from ionized particles decrease
- the amount of information that can be modulated onto the carrier increases in roughly linear proportion

Name of Range	Abbreviation	Frequencies
High Frequency	HF	3 - 30 MHz
Very High	VHF	30 - 300 MHz
Ultra High	UHF	300 - 3000 MHz
Super High	SHF	3 - 30 GHz
Extremely High	EHF	30 - 300 GHz
Infrared		300 GHz - 300 THz
Visible Light		300 - 900 THz

Table 1. Typical Grouping of Carrier Frequencies

- sensitivity to atmospheric scintillation caused by nuclear bursts decreases.

The impact of these basic effects on performance will be discussed in detail in the following paragraphs.

1.2.1.1. Long-Distance Atmospheric Transmission

Energy from the sun ionizes molecules in the upper atmosphere, creating a band of plasma commonly called the ionosphere. This band is characterized by its plasma frequency, essentially the composite resonant frequency of the ions in the plasma. This plasma frequency varies with time of day, month, and year, and can thus only be approximated over any given length of time. This frequency is of interest, for incident radiation at frequencies below the plasma frequency will be reflected. This effect makes over-the-horizon radio communication possible.

Over-the-horizon communications will be of increasing importance in the future tactical theater because of the increasing size of the theater. The distance between the sustaining base and the FLOT may be several hundred kilometers in the central European theater, requiring the transmission of a substantial amount of information using some form of over-the-horizon communications.

Unfortunately the atmospheric channel is limited in a variety of areas. Reliable long distance radio communication is possible with carrier frequencies up to a maximum of approximately 20 Mhz. Carrier frequencies are thus limited to the HF and low VHF ranges. Frequency selective effects will then limit instantaneous bandwidths to approximately 1 Mbps. Susceptibility to enemy action is correspondingly severe. Passive interception is extremely easy. The ionosphere scatters the signal as it reflects, creating a broad area in which successful reception is possible. Passive interception is also undetectable. This is worthy of note because such interception is always detectable in some of the other media. In the over-the-horizon channel heavy reliance must be placed on encryption. Active interception is also highly probable, because it is difficult for the receiver to get an accurate idea as to the origin of any given signal. Again, heavy reliance must be placed on encryption.

The worst problems arise in the area of disruption. Disruption can take a variety of forms, including the bombardment of communications equipment, jamming, and sabotage. In the tactical arena, particularly in areas close to the FLOT, the first two forms of disruption listed here present the greatest threat. To characterize the threat one must take into account the Soviet battle plan³. Soviet tactics emphasize brute force and avoid sophistication wherever possible. If this somewhat simplistic rule of thumb is applied to the disruption of HF and VHF over-the-horizon communications, the following conclusions readily follow. Communications will be interdicted whenever possible through the destruction of equipment by 1.) identifying the critical components, and 2.) directing an overwhelming amount of artillery in the appropriate direction. These achievement of these two objectives is probably easier with an over-the-horizon communication system than with a system using any other medium. An OTH transmitter produces a large electromagnetic signature that can be used for both traffic analysis (objective 1) and targeting (objective 2). Narrowbeam systems are difficult to construct at these frequencies because of the relationship between frequency, beamwidth, and antenna size. A reduction in electromagnetic visibility will result in an increase in optical visibility.

The other method of disruption involves jamming, or denying the use of the channel to anyone. There are two types of jamming that must be considered: broadcast noise and scintillation caused by a nuclear explosion. Broadcast noise can be countered through the use of spread spectrum techniques. Such techniques use additional

frequency spectrum to force the jammer to spread his noise over a wider range. The goal is to reduce the ratio of noise power to signal power at the input to the receiver. Jamming strategies in the academic world can be extremely sophisticated (fast frequency followers, tone jammers, comb jammers, and the like), but at these low frequencies such techniques will not be necessary. The available bandwidth at HF and VHF frequencies is very restricted. The brute force utilization of a large number of "dumb" noise generators should prove to be more than sufficient.

Should a tactical engagement escalate to the use of nuclear weapons, a second and much more effective form of channel disruption becomes possible. An above-ground nuclear explosion creates a burst of energy that ionizes the atmosphere in much the same manner that the energy from the sun creates the ionosphere. Unfortunately this is too much of a good thing. The extreme level of ionized radiation causes a scintillation effect, scattering electromagnetic radiation passing through the area. Received signals suffer from deep fading and phase jitter. The duration of this effect is inversely proportional to the frequency of the transmitted signal. HF and VHF signals are severely affected for hours.

1.2.1.2. Line-of-Sight Transmission

If propagation requirements are reduced to line-of-sight distances, then much higher frequencies can be used. UHF through EHF radio transmission becomes a possibility, as does optical communications. The higher carrier frequencies provide a host of positive benefits:

- reduced scattering effects place a greater burden on intercepting receivers; they must be more carefully placed to receive the signal
- detection and interception can be made even more difficult through the use of highly directional antennas. As carrier frequency increases, the size of the antenna necessary to achieve a given beamwidth decreases. It is thus much more practical at higher frequencies to employ highly directional communication links. Higher directionality also makes targeting by ARM's much more difficult.
- all of the foregoing also make active interception more difficult as well

- the duration of scintillation induced channel fading decreases to a few seconds with EHF communications
- placement of jammers becomes a much more critical problem for the enemy. The impact of geometry on the jamming problem is proportional to the carrier frequency.
- the availability of additional bandwidth leaves more room for spread spectrum techniques, making jamming more difficult.

The negative aspects of these higher frequencies must also be considered.

- The resonant frequencies of oxygen and water molecules lie in the SHF and EHF bands. As center frequencies approach these frequencies, the absorptive effects of the atmosphere become more pronounced, increasing the required transmitter power for communication over a given distance⁴.
- Optical communications are highly sensitive to local terrain effects (trees) and particulates in the air (dust).

1.2.1.3. Sub-Orbital Platforms

Airborne communication platforms can be used as relays to achieve over-the-horizon communications. If the platform is within sight of both the source and destination of a given transmission, then virtually any communication medium can be used. The positive aspects are as follows:

- Ground units can use tightly focused EHF or optical channels to communicate with the platform. The units will thus be relatively safe from detection.
- Platforms can be provided with highly directive antennas (e.g. steered phased arrays with adaptive nulling) that will reduce susceptibility to jamming.
- Platforms can be easily moved to accommodate changes in the battle.

The negative aspects are as follows:

- Airborne platforms must be launched from a relatively secure position. If this involves the use of an airfield deep within the sustaining base, deployment will be slow.
- Airborne platforms used as relays are extremely visible in both an optical and electromagnetic sense. In the highly lethal tactical battlefields of the future the expected lifetime of the platform will be short. A great deal of redundancy must be provided.

1.2.1.4. LEO Satellite

Low earth orbit satellites can also be used to provide a relay function for over-the-horizon communications. Depending on the orbit, the satellite will be in view for anywhere from 90 minutes to several hours. The longer the visibility, the higher the orbit and the greater the expense of deployment. Clearly several such satellites must be used to ensure complete coverage and survivability. LEO satellites are harder to knock out than airborne platforms using conventional weapons. However, a well placed nuclear burst can be used to induce EMP in a satellite several miles away, effectively destroying the electronics within the satellite.

1.2.1.5. Geosynchronous Satellite

Geosynchronous satellites are extremely difficult to knock out and almost as difficult to replace. They also suffer from a 478 to 556 millisecond round trip signal propagation delay that could be a critical problem for some forms of communication (e.g. weapons guidance).

1.2.2. Propagation through Confined Channels

We define "confined channels" as those that involve the deployment of media such as copper wire or fiber optical cable. The characteristics of such channels are markedly different from those of the atmospheric/free space channels. The first and most obvious of these differences is the increased difficulty involved in deploying the channel. The difficulty is not, however, as pronounced as one might initially imagine. The development of wire guided missiles and bombs (e.g. the Maverick missile) has considerably advanced the art

of laying out cable at an extremely high rate of speed. Land vehicles (HUMV) and helicopters are currently used to lay out copper wire between communication hubs on the battlefields of the 1980's. By the year 2000 it is safe to assume that techniques will be available for deploying fiber optical cables at very high speeds. So though the deployment of confined channels is more difficult, it is clearly not an insurmountable problem. The positive aspects of such channels in a tactical scenario are impressive. Consider the following:

- The enemy can passively intercept communications on confined channels through the use of couplers. The couplers drain off a very small portion of the transmitted signal without altering the performance of the channel to any significant degree. However, in doing so the coupler causes a reflected delayed image of the signal to appear at the transmitter. Time domain reflectometry techniques can then be used on both wire and fiber optical channels to determine the exact location of the coupler. Active interception is even more readily detected, because it necessitates the termination and regeneration of signals moving through the channel.
- Confined channels allow for a high degree of spatial diversity. Multiple cables taking multiple routes can be used to connect two sites. The enemy must destroy all of the cables before communication can be disrupted.
- Communications systems making use of confined channels can be operated at much lower power levels. This translates into lower size, weight, and cost of the equipment.

The negative aspects of confined channels are readily apparent.

- A significant amount of damage to the cables must be expected from armored vehicles and the like.
- Mobile communications are practically impossible using confined channels.

The following subsections cover some of the specific attributes of wire and fiber optical channels.

1.2.2.1. Wire

Wire channels include twisted pairs of copper wire and shielded coaxial cable. This medium can be used at center frequencies up to a few hundred megahertz before the skin effect increases the resistance of the wire to an unmanageable level. The available bandwidth is thus limited. The principal problem with wire channels in the central European theater will come into play if the conflict escalates to the use of nuclear weapons. Nuclear weapons produce a burst of electromagnetic radiation. When this burst encounters a conductive material, it induces an electromotive force which in turn causes a current to flow through the wire. This resulting system generated electromagnetic pulse (SGEMP) can completely destroy the communications equipment at both ends of the wire. It is possible to design protective circuits to guard against this phenomena, but some amount of rebuilding will always be necessary after each nuclear burst.

1.2.2.2. Optical Fiber

Fiber optical channels offer enormous amounts of bandwidth and may thus prove quite useful for virtually all type of fixed communication on the tactical battlefield of the future. Optical fiber enjoys all of the benefits of wire, but does not suffer from the aforementioned problems of limited bandwidth and SGEMP (fiber optical materials do no conduct electricity and are thus not subject to the Faraday effect).

1.2.2.3. Recording Media

NATO emphasizes that transfer of data on recording media should not be overlooked⁵. This medium provides for arbitrarily large bandwidth, but also instills tremendously larger delays than other media. It also provides increased security through human supervision of the data being transferred. It is expected, however, that if a properly functioning communication system is in place, transferring data via recording media will be much more expensive than transfer through the system.

1.2.3. Multi-Media Switching

It is clear from the foregoing discussion that the various media available for use in a tactical communication system provide distinct positive and negative attributes. It is possible to reinforce the

positive while reducing the impact of the negative through the use of media switching. A primary medium is selected for a system based on a series of trade studies. The primary medium is supported by secondary and possible tertiary media whose role is to enhance survivability and maintain connectivity.

Consider the case of a trunk line between the FLOT and a rear area in the sustaining base. The primary medium would most likely be a series of fiber optical cables. If too many of the individual cables are destroyed, the system would revert to a secondary medium such as an HF OTH link, while the tertiary medium might be an EHF satellite link. Each of these three media offers significantly different strengths and weaknesses; thus an environment that precluded the use of one medium might readily allow the use of the other two.

The Air Force is currently developing a multi-media resource manager⁶ whose task is to actively switch channel usage between a variety of media in response to enemy action.

1.3. Data Encryption Options

The importance of good data encryption in military communications systems was recognized by the Greeks well before the time of Alexander. In a tactical environment it must be assumed that at some point the enemy will intercept one or more transmitted messages⁷. As noted earlier, some media are more susceptible to interception than others. For the content of the messages to remain secure, they must be written so as to only be intelligible to the intended recipient. This is accomplished through the use of cryptographic techniques. The science of Cryptology has advanced rapidly since the introduction of the rotor machines used in World War Two. One can now state with mathematical certainty that a message encoded with the aid of a simple personal computer cannot be broken by the enemy within the time constraints of a tactical engagement without the use of side information (e.g. the key)⁸. The military cryptographic problem has thus evolved from one of creating codes that cannot be broken to one of preventing access by the enemy to the key. This is an important consideration because the mobility and turmoil of a tactical theater make the key distribution problem a particularly difficult one. Two approaches to the problem of key distribution will be examined in the following pages. Before proceeding it must be noted that the data security issue is not just a matter of keeping the enemy from reading friendly mail. The following must also be considered:

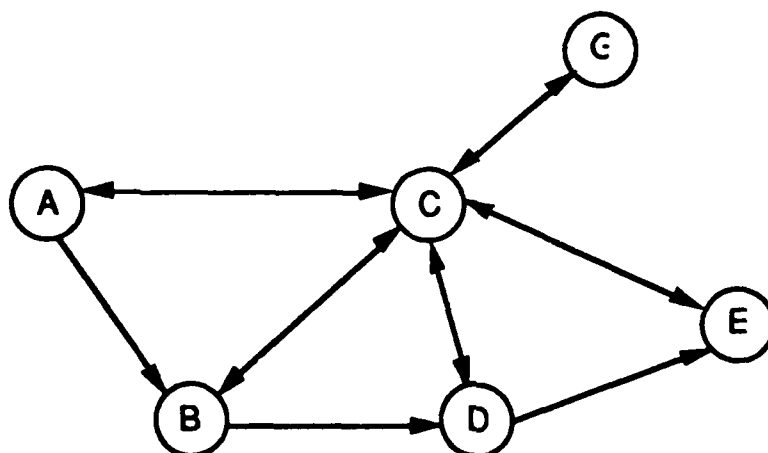


Figure 2. A Simple Network

- Traffic patterns can be determined without actually decrypting transmitted messages. Such patterns can be used to predict troop movements and the location of headquarters at various levels.
- It may be necessary to implement several levels of classification for messages in the network. This creates a routing problem, for messages of the highest classification must be routable by nodes with the lowest classification to maintain complete connectivity on the network.

Consider the simple network shown in Figure 2. If each node generates the same amount of message traffic with equiprobable destinations, then node C will be much busier than the other nodes. If the enemy was able to recognize this, then they could severely reduce the performance of the network by concentrating their offensive firepower on node C.

Several methods can be used to mask traffic patterns on the network, including the use of empty message frames or tokens throughout the network (all nodes are thus equally busy, though some of the messages processed are blank). These upper level considerations will be discussed later in the report.

The problem of maintaining multiple classification levels on a network is much more difficult. End-to-end encryption is quite adequate for protecting the data field within messages. This does not, however, protect information on high level classified traffic from

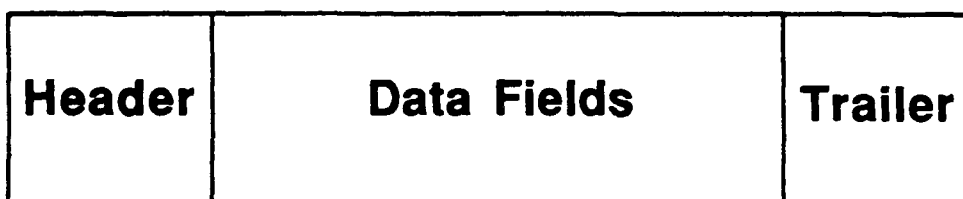


Figure 3. Generic Packet Structure

lower level users. Header fields must be readable to some extent to allow for efficient routing. Several methods exist for solving this problem as well. One possibility involves dividing the header up into multiple subheaders. Each node reads only its own designated subheader and switches the message accordingly. The subheaders are encrypted at the classification level of the associated node. The ultimate destination of the packet, however, cannot be determined without decrypting all of the subheaders.

The selection of individual security codes depends on a variety of factors. The first and foremost is the degree of redundancy to be expected in the unencrypted data.

Consider the generic packet shown in Figure 3. Header information usually follows a well-defined format. The length of the header is minimized to reduce overhead, thus any conceivable combination of header bits will be meaningful (i.e. there is no redundancy). In this situation absolute security can be obtained by simple monophonic substitution. The data field presents another problem. Uncompressed English language text contains a great deal of redundancy. It is thus easy to tell whether an attempt at decryption has succeeded or not. If the result is readable, then chances are that the decryption has succeeded! The codes selected must thus be much more sophisticated than simple substitutions. Happily there exist several encryption schemes that are virtually impossible to break without several weeks of work by a supercomputer.

It is clear that the current state of the art in Cryptology will be sufficient for data protection in the post-2000 battlefield. The problem will lie in carefully selecting the right codes and the means of key distribution. We return to the latter problem because it is both the most straightforward and the most important. The recent development of public-key cryptography may provide a solution.

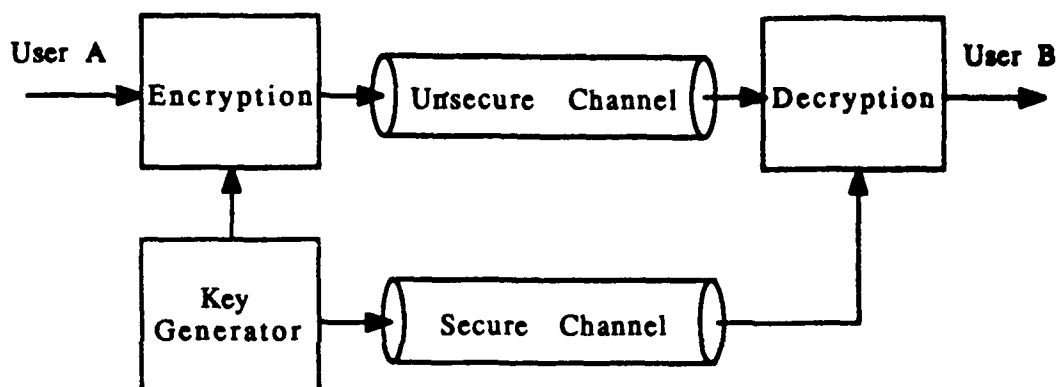


Figure 4. Private Key Encryption

1.3.1. Private Key Encryption Techniques

All of the encryption techniques designed from the beginning of time up until 1976 can be categorized as private key systems. Such a system is characterized by a single key that is known to both parties who wish to communicate. The implementation of the system requires the selection of the key by one party and the transmission of the key to the other party by way of a secure channel, as shown in Figure 4. In tactical situations the secure channel usually takes the form of a courier. On the battlefields of the future it may be possible to use confined channels that are known to be free of eavesdroppers. Verification of security can be obtained through careful use of time domain reflectometry.

Cryptosystem keys are created for specific missions and distributed to the appropriate personnel. After a short period of time the keys are destroyed and the process is repeated. The useful lifetime of the key is limited because of the following:

- during the course of the battle codebooks can be lost or captured
- the more encoded material the enemy has, the easier it is for them to determine the key (as noted earlier, this is not as much of a problem as it used to be).

The problem of private key distribution is thus extremely important. The tactical environment of the next century will in all probability make it even more difficult.

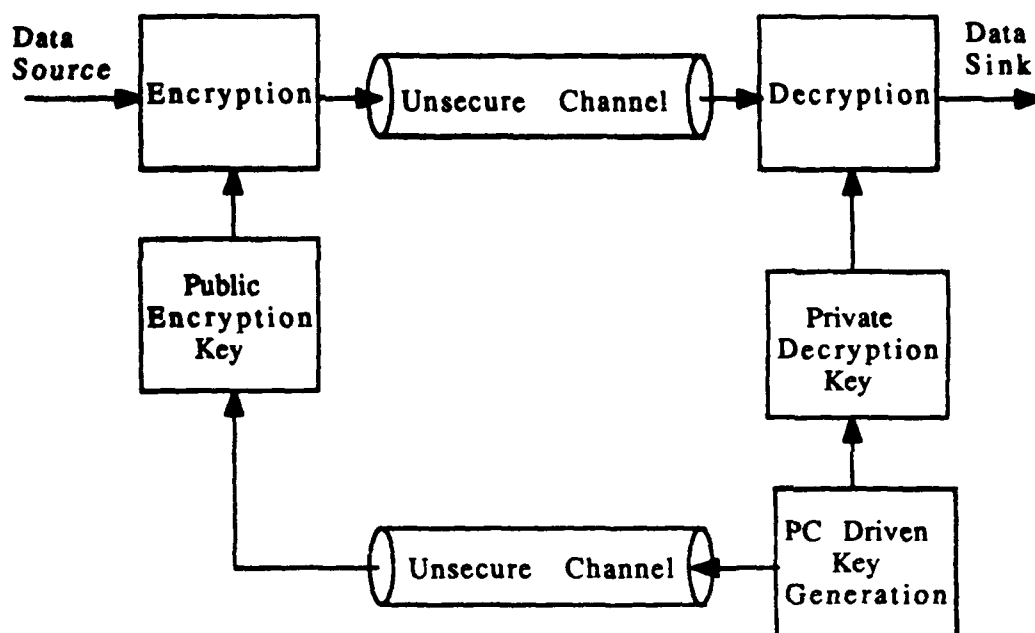


Figure 5. Public Key Encryption

1.3.2. Public Key Encryption Techniques

Public key cryptography was first described by Whitfield Diffie and Martin Hellman⁹. The encryption process involves the creation of two keys for each user: one key for encryption, the other for decryption. If the goal of the encryption process is to render information illegible to all but the intended recipient, then the encryption keys are published in a phonebook available to all while the decryption keys are kept secret by the individual users. If user A wishes to communicate with user B, he looks up User B's encryption key in the public phonebook. Since only user B has the ability to decrypt the message, the information is secure. A generic system is shown in Figure 5.

This two key system is based on the use of one-way trapdoor mathematical functions. Such functions are easy to perform in one direction and extremely difficult to do in the other. Examples include exponentiation and logarithms in finite fields. The encryption process is then constructed from the "easy" direction and the decryption from the "difficult" direction. The function is "trapdoor" if the difficult operation can be made easy through the use of side

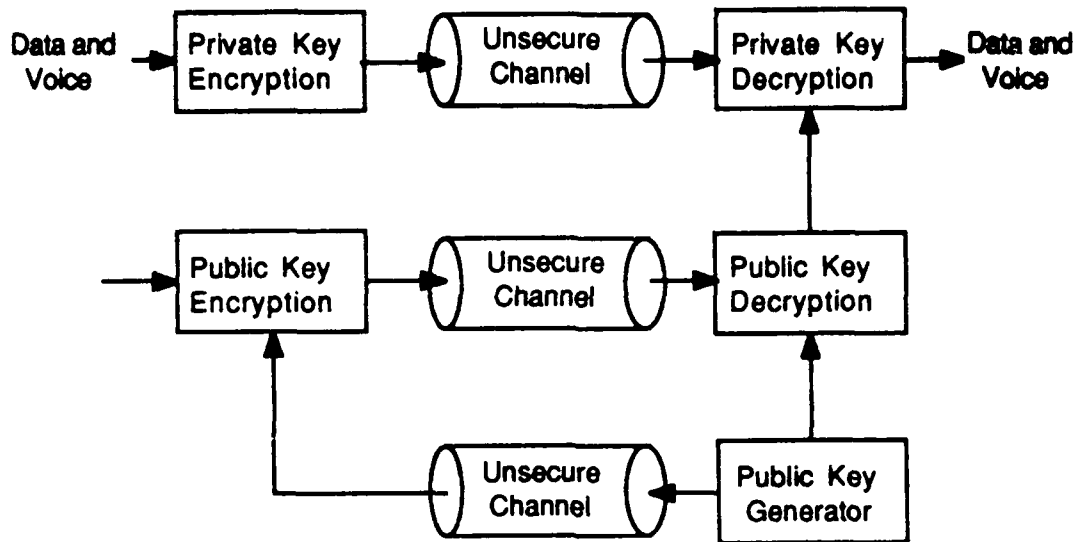


Figure 6. Combined Public/Private Key Encryption

information. The private key kept secret by each user contains the necessary side information for easy decryption.

Several specific schemes have been proposed by a variety of authors. In all of these schemes the private decryption key can be generated on location by the individual users. Communication is made possible by the exchange of public encryption keys. There is thus no need for a secure channel for the exchange of keys. The key distribution problem is thus vastly simplified.

Public key encryption also allows for authentication of information, something that is extremely difficult to do with private key systems. In public key authentication the encryption key is kept secret while the decryption key is published. Thus all users can decrypt and read the "signature" but only the user with the encryption key can generate it.

1.3.3. Combined Public/Private Key Systems

The principle disadvantage of public key systems is their speed. A public key system based on the RSA algorithm may be able to run at 10 to 30 Kbps, while the private key DES protocol can be readily implemented at T1 (1.544 Mbps). The best of both worlds can be obtained by combining the two approaches. Public key algorithms can be used to distribute keys for a private key encryption system. The key and all subsequent information may thus be transmitted

over unsecured channels while communication is possible at the higher rates typical of private key systems. The basic scheme is depicted in Figure 6.

1.4. Communication Subnet Architectural Alternatives

1.4.1. Fundamental Choices

The communication subnet includes the Physical, Logical Link, and Network Layers of the communication architecture. While there may appear to be innumerable architectural alternatives for a subnet, a closer examination shows a natural division into a fairly limited set of basic options.

The architectural alternatives are divided as shown in Figure 7. While most contemporary taxonomies divide the architectures first by application (i.e., Local Area Networks, Wide Area Networks, etc.), a consideration of far term implementations requires a taxonomy that is driven not by current methods, but by fundamental features.

The taxonomy is first divided into Single-Hop and Multi-Hop systems. A network will be defined as Multi-Hop if routing decisions are made while traversing the network. An immediate consequence of this is the potential for queueing of data at various points in the network. This necessarily increases the complexity of network equipment, since problems of topology design and maintenance, routing, and flow control must be addressed if the network's resources are to be used efficiently.

Networks where routing decisions are not made while traversing the network will be referred to as Single-Hop networks. The architectures utilizing this approach that have appeared in the literature can be classified as:

- point-to-point links
- broadcast through confined channels
- broadcast through atmospheric channels
- single-repeater systems
- directional propagation through confined channels
- rings
- double rings.

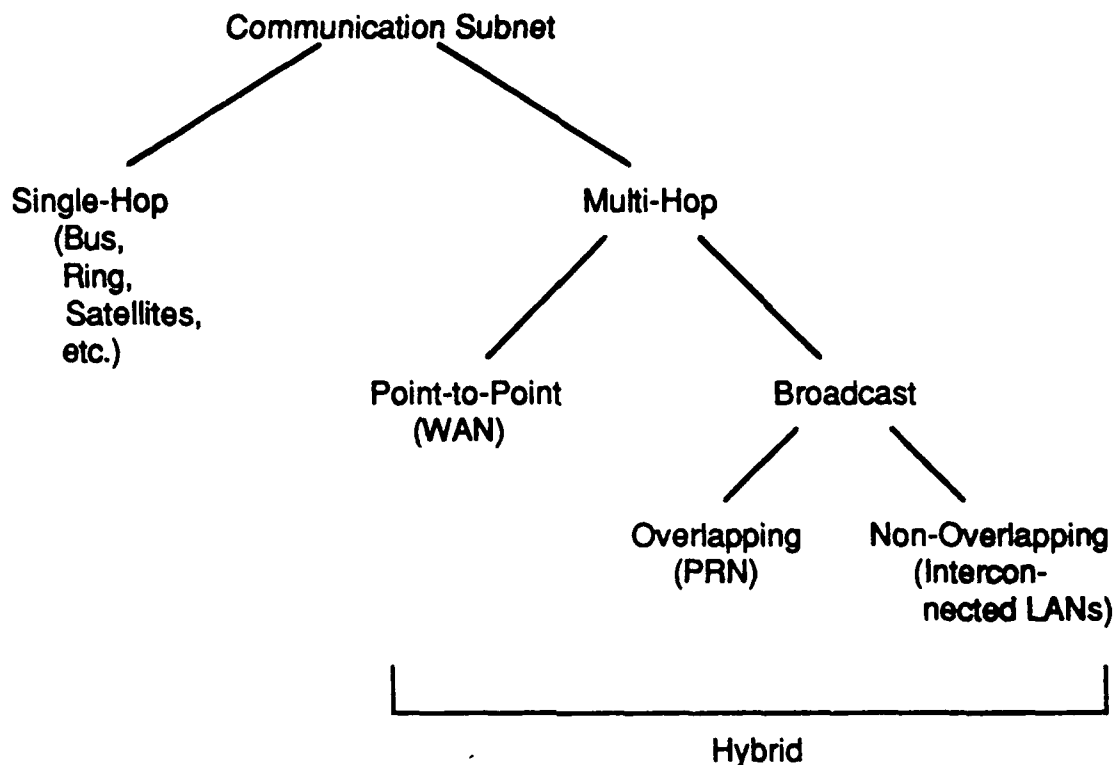


Figure 7. A Taxonomy of Architectural Alternatives

Multi-Hop networks can be further classified according to whether the media consists of point-to-point channels or broadcast channels. When point-to-point channels are used, a mesh of links results. When broadcast channels are used, the structure depends on whether the recipients of a broadcast can be divided into distinct groups. If they can, the broadcasts will be said to be non-overlapping. If they cannot, the broadcasts will be said to be overlapping.

An additional alternative with broadcast networks is a hybrid combination of point-to-point links, overlapping broadcasts, and non-overlapping broadcasts.

Each of these alternatives will be examined in turn, and the basic characteristics of each will be identified.

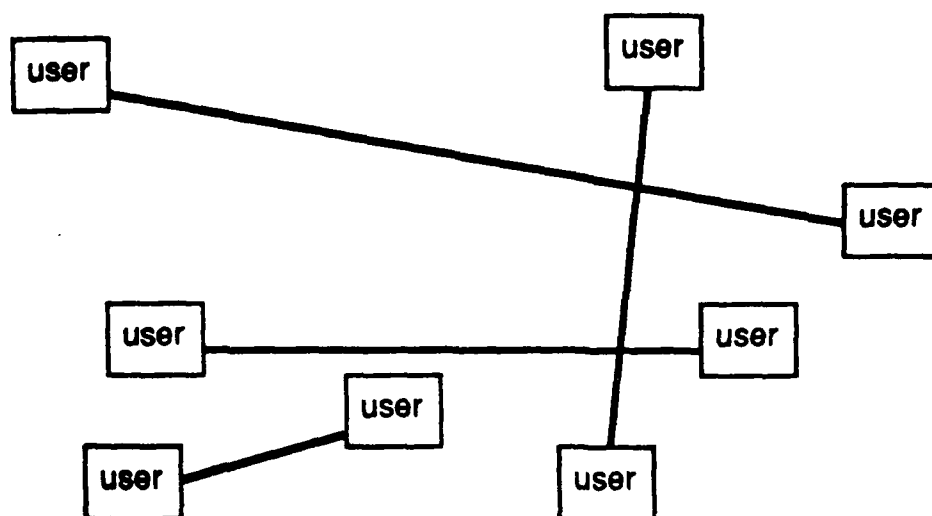


Figure 8. Single Point-to-Point Links

1.4.2. Single-Hop Networks

1.4.2.1. Single point-to-point links

In these systems each pair of users has a dedicated point-to-point connection, as illustrated in Figure 8.

There are no meaningful issues above the physical layer with point-to-point channels. By definition, the channel is set up for exclusive communication between two well-defined points, so there can be no contention.

1.4.2.2. Broadcast through confined channels

With a broadcast system, all users communicate through a single shared medium, and each user listens to each transmission, discarding packets for which it is not the destination. The topology is shown in Figure 9.

The main characteristics of broadcast through confined channels are:

- a wide variety of access methods may be used, ranging from very simple, inexpensive methods to highly sophisticated methods providing almost any desired operational behavior

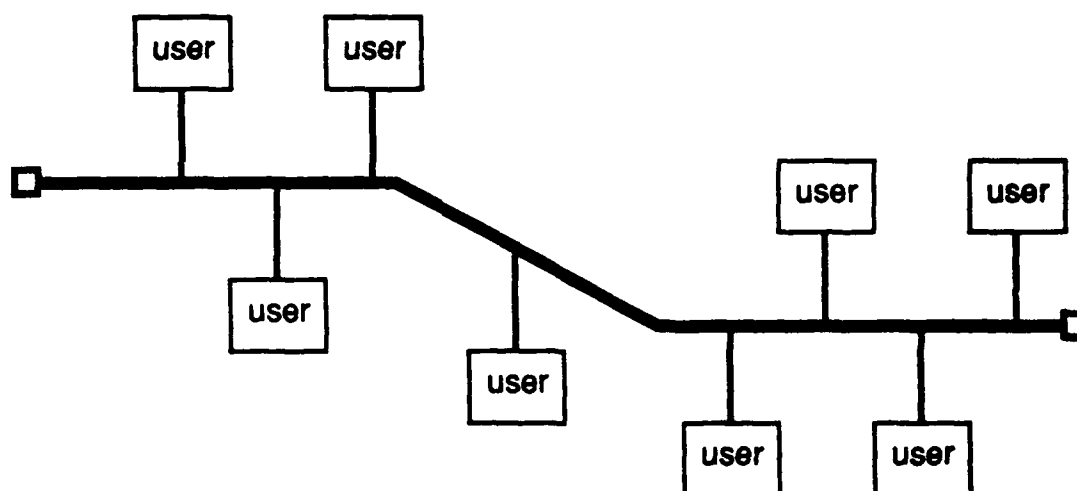


Figure 9. Broadcast Through a Confined Channel

- there is a fundamental limit on the performance of the system as a function of the maximum propagation delay in the system, the data rate, and the mean packet length

The limitation on performance caused by the determination of access. While a precise upper bound depends on the nature of the implementation, a rough bound can be given as

$$\text{upper bound on channel utilization} \approx \frac{1}{1+a}$$

where

$$a = \frac{(\text{data rate})(\text{average propagation delay})}{(\text{average packet length})}$$

Here channel utilization is defined as the portion of time data is sent on the channel.

Since the average propagation delay and average packet length are usually determined by the application, the result is a decreasing channel utilization with increasing data rate, as illustrated in Figure 10.

Upper Bound on Channel Utilization for a Broadcast Bus

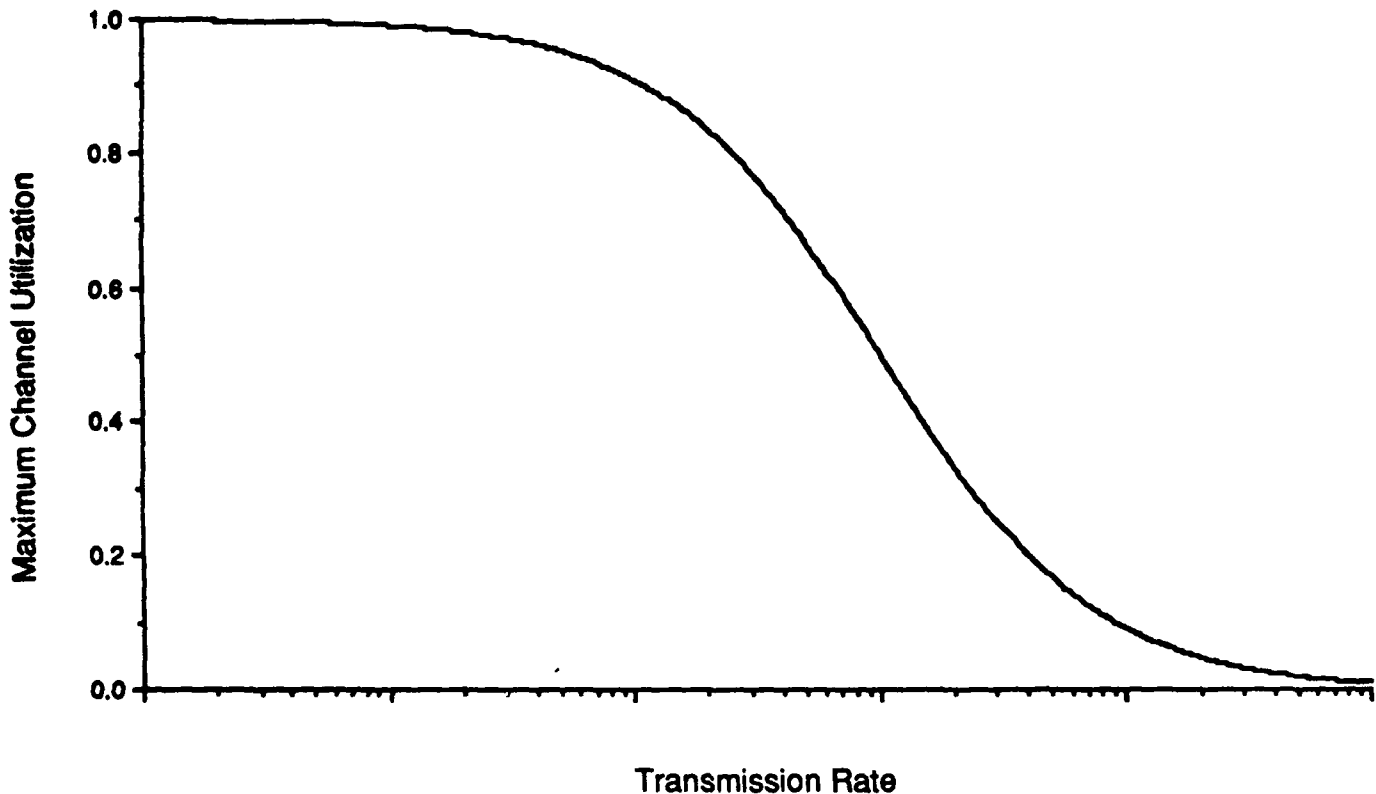


Figure 10. The Relationship of Transmission Rate to Maximum Channel Utilization on a Broadcast Bus (Note: the horizontal scale is logarithmic)

Broadcast busses have been a popular choice for contemporary local area networks. Simple access has provided for inexpensive access devices, and the small system diameter has abided the limit on performance. But as data rates increase, the applicability of broadcast architectures will be reduced. This can be alleviated partially by artificially lengthening packets through frequency or code division techniques, but the fundamental limit still leaves the long-term viability of broadcast networks in doubt.

The survivability of broadcast bus systems depends partially on their implementation. For most access protocols, the elimination of one or more users does not reduce the ability of the remaining users to communicate. The effect of physical disruption of the channel depends on the medium used. With electromagnetic connections, the lack of proper termination can be expected to prevent further use of the channel. If an optical medium is used, however, termination is

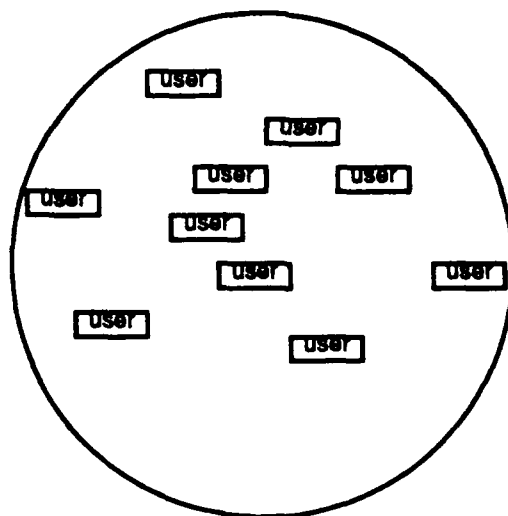


Figure 11. Broadcast on Atmospheric Channels

not a problem, and segmented portions of the network may still act as individual networks.

1.4.2.3. Broadcast on Atmospheric Channels

In this architecture, several users use radios to communicate in an environment where all users can hear all transmissions. The architecture is illustrated in Figure 11 (Note: the circle represents a constraint on the maximum distance between users; the users do not necessarily have to lie within a circle.).

The use of a single broadcast channel has most of the advantages and disadvantages of broadcast on a confined channel. It also has the additional characteristic of susceptibility to disruption and traffic analysis.

A broadcast bus may be the only viable option in an environment where users cannot be interconnected by wires or optical fibers.

One extreme case of this is the current JTIDS system, where broadcast over an entire theater is achieved through a combination of time division, frequency division, code division, and very low data rates.

1.4.2.4. Single-Repeater Systems

In a single-repeater system, all users send outgoing data to a central repeater. The repeater broadcasts what it hears to all users. The

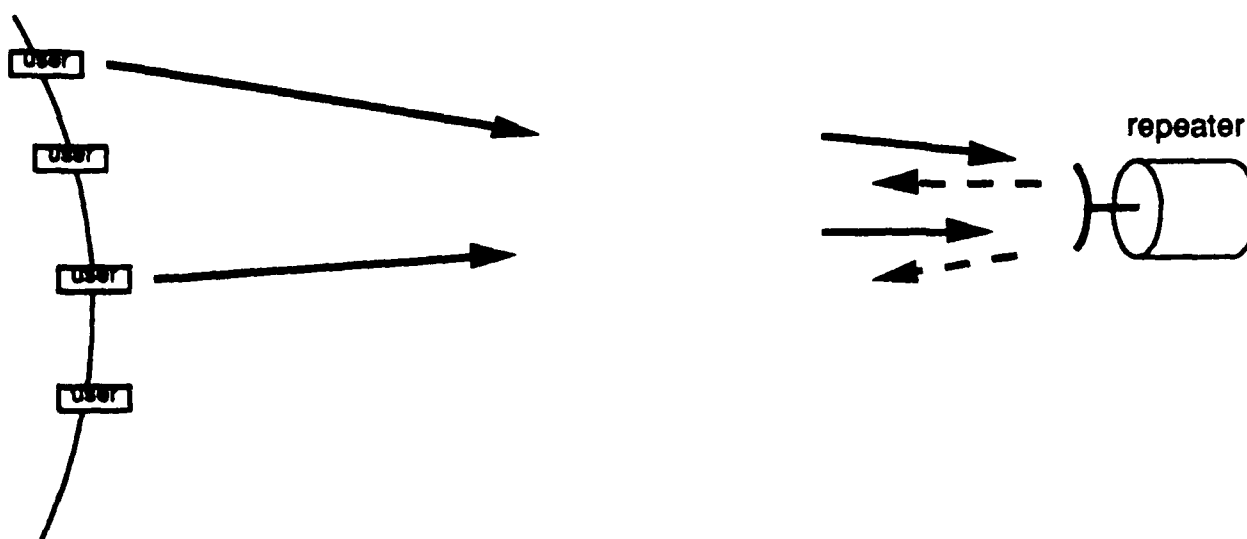


Figure 12. A Single Repeater System

most typical implementation of this architecture is satellites, as illustrated in Figure 12.

The survivability of single repeater systems is limited by the survivability of the repeater. As the survival of the system rests on a single component, the survivability of the system can be assumed to be poor.

Since geosynchronous satellites present some special characteristics, it will be discussed in a separate section. A discussion of other systems will follow.

1.4.2.4.1. Geosynchronous Satellite Access

Satellite access among several users may involve contention. Geosynchronous satellites have the added factor that a round-trip delay of roughly 250 milliseconds will occur with all transmissions, so that knowledge of a collision will occur well after the transmission of a packet has been completed.

The typical limiting factors in satellite usage are:

- the bandwidth of the repeater
- the footprint and power requirements for communication
- susceptibility to jamming and interception
- susceptibility to weather conditions

There are a variety of approaches to satellite access, for which the basic parameters are:

- the number of possible contending users
- the available bandwidth
- the statistical nature (data rate, duty cycle, etc.) of the data to be transmitted

The techniques used for access can be broken into the elements, often used in conjunction, of

- time division
- frequency division
- code division
- random access (with contention)
- reservations (Demand Assignment)

Each of these factors can be viewed individually according to their characteristics.

Division of time among users requires additional hardware for users to synchronize to each other, or at least to the satellite. If used in isolation, a very low utilization can result from users with a low duty cycle.

Division by frequency can have some of the same problems as division by time, except that synchronization among the users is not required. One additional problem is that users must be able to receive on any of several frequencies, so full connectivity requires more demodulators.

Division of bandwidth by coding methods has some inherent advantages over frequency and time division, but also some disadvantages. Coding provides simpler connectivity than the other methods, and provides inherent jam resistance. An important negative is that the use of bandwidth tends to be much less efficient than with other methods.

Random access on satellites is limited by a propagation delay much longer than the length of a packet, so that users become aware of collisions long after they occur. The main method for random access with a large number of users is an ALOHA method, which has a

maximum effective utilization of bandwidth of only 18% (or 36% if the users are time-synchronized).

One means of improving bandwidth utilization in random access satellites is the use of reservations. The central idea is that only a small portion of the system is used for contention, so that most of the bandwidth remains available for transmission of data. Numerous reservation methods have been suggested.

The survivability of geosynchronous satellites in the far term is difficult to predict. Some argue that the very high altitude, coupled perhaps with reflective paint, will provide adequate protection against destruction. Others argue that the ease of locating geosynchronous satellites will make them highly vulnerable. NATO documentation suggests that the cost and limited availability of satellite communications is likely to curtail significant use at the tactical level, but that it may be present for special purposes¹⁰.

1.4.2.4.2. Other Single-Repeater Systems

Other implementations of single-repeater systems include low altitude satellites, and terrestrial systems using a head-end as a repeater.

Low altitude satellites have the characteristic of periodically entering and leaving the zone where they are useful for orbit, and thus require special methods for the Physical and Logical Link Layers. Methods have been developed that appear to be fully effective¹¹.

Access methods with these system may be the same as for geosynchronous satellites, or may correspond to methods used on broadcast busses.

The survivability of these systems can be expected to be less than that of geosynchronous satellite systems, as the repeater will be much easier to reach.

1.4.2.5. Directional Propagation on confined channels

A number of architectures based on unidirectional propagation along one or two parallel channels have been proposed. Examples in the current literature include DATAKIT, FASNET, QPSX, EXPRESSNET, and others. One possibility is illustrated in Figure 13, where users send data on the channel, and receive it again on a second pass of the channel.

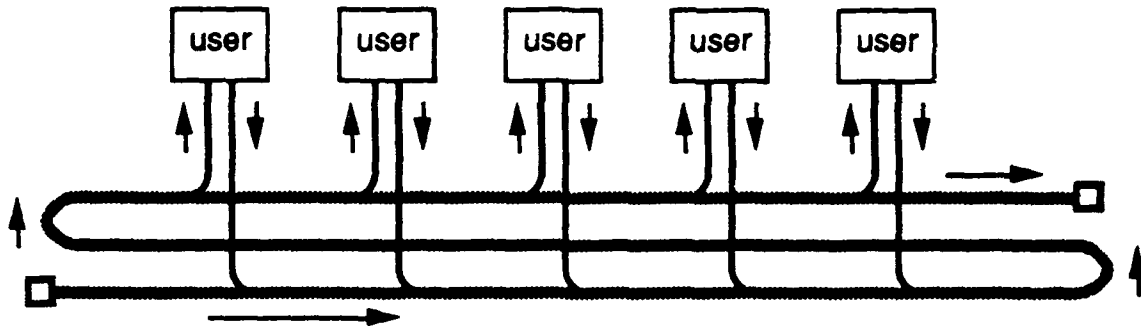


Figure 13. An Example of a Network Using Directional Propagation on a Confined Channel

These systems overcome the limitations on performance at high data rates present on broadcast busses, and are excellent candidates for local area network architectures in the far-term.

The survivability of these systems is poor, as a break in the channel at any point will bring the system down.

1.4.2.6. Rings

A ring has been described as the topology that arises when each user has exactly one input line and one output line, these are connected so all users are attached to each other, and the system is picked up and shaken out. The topology is shown in Figure 14.

The important characteristics of rings are that:

- they are simple
- performance is limited by the number of users and the circumference
- they are easily implemented with a fiber optic cable
- their survivability is rather poor.

The simplicity of rings and their ease of implementation with optical fiber have motivated their contemporary use in local area networks.

The performance of the ring depends partially on the media access method, but is generally limited by the number of users and the propagation delay around the ring. With increasing complexity, however, the latter limitation can be overcome¹². The diameter

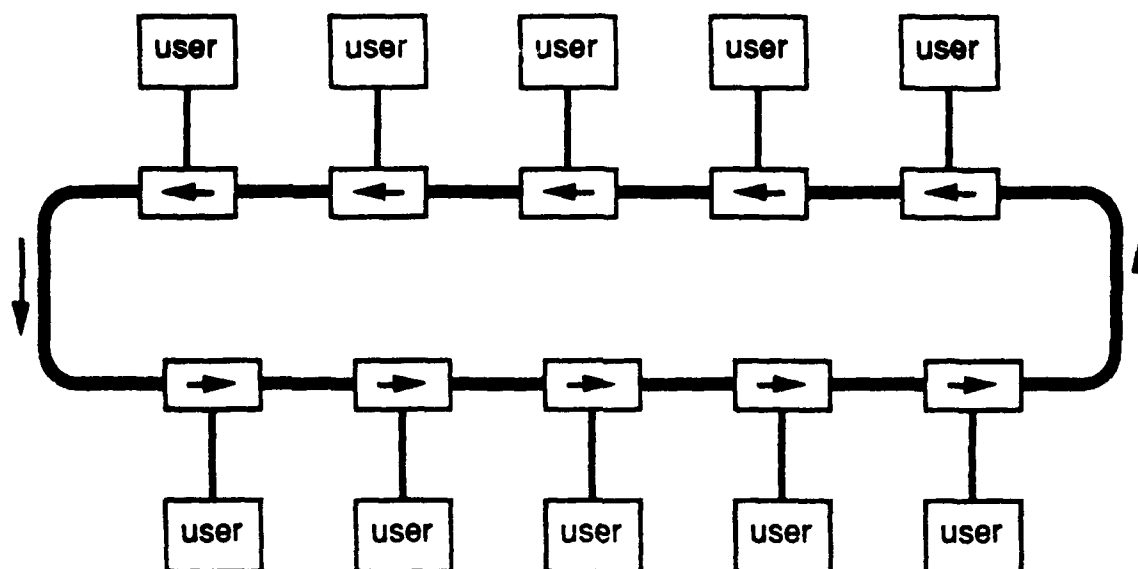


Figure 14. A Ring Topology

supportable by a ring tends to be larger than for bus networks serving data at the same rate.

The poor survivability of rings has been a problem even in relatively benign commercial implementations. While several methods for improving the survivability have been found, they have generally required mechanical switches or constraints on the physical layout of the cables. The cost-effectiveness of these solutions have been doubtful.

1.4.2.7. Double Rings

Double rings are a variation on the ring topology intended to increase survivability. The usual implementation is to have two rings with identical physical cabling, but with data transferred in opposite directions.

This has advantages on performance greater than the simple doubling of capacity, since a source can send its data to a destination in the "shorter" direction (although this advantage may be removed by the access method, as data must sometimes pass all the way around a ring, anyway).

The double ring is significantly more survivable than a single ring. A loopback can be inserted on either side of a break in the network, effectively turning the double ring into a single ring structure.

Multiple breaks can be treated similarly, with the system segmented into several smaller rings. This capability requires active components to provide the looping as needed, and complete connectivity is lost with two or more breaks. Thus the survivability of rings is enhanced, but remains limited.

Double rings have been implemented as Metropolitan Area Networks, as can be seen in the FDDI architecture.

1.4.3. Multi-Hop Networks

1.4.3.1. Topologies

One of the first problems in the implementation of a multi-hop network is the choice of topology. Topology design may be driven by operational concerns, such as sufficient connectivity for adequate survivability, as well as performance issues.

One of the topological concerns that overlay the entire network is the question of whether it is better to have one big network capable of handling all types of data, or to have several smaller networks designed for specific applications. The current trend in civilian communications is to integrate various data types onto single networks, with the belief that the added complexity of handling different types of data is far outweighed by the cost advantages of a single management structure and the performance advantages of sharing resources among a greater number of users. The motivation is enhanced in a military setting by the much greater connectivity provided by integrating services onto a single network.

1.4.3.2. Circuit-Switching, Packet-Switching, and Alternatives

One of the fundamental questions that must be addressed in any communication system is the organization of the switching of media.

The earliest alternative that was developed was circuit-switching, where a channel composed of a number of interconnected circuits was set up at the beginning of a call, reserved for a particular pair of users, and released when the call was finished.

The next alternative that was developed was packet-switching, which organized data into convenient "packets," each of which was sent through the network as a unit. Packets could share media by queueing if a particular circuit was in use when it was ready to be

sent. This provided for much more efficient channel use, and the cost of less certain delays for individual packets.

More recent alternatives include systems which provide a variety of media characteristics and alternatives, according to the type of data sent.

1.4.3.3. Routing

For networks of point-to-point channels, the problem of routing is fairly well understood even today¹³. The problem of routing can be divided into the issues of routing of datagram traffic and routing of virtual circuit traffic.

The problem of routing in packet radio networks is still a subject of significant research, and the current rate of progress indicates that significant gains are yet to be made in this area.

1.4.3.4. Flow Control

Network layer flow control attempts to throttle the rate of traffic entering a network so that the network can operate effectively. Experience has shown that a network without effective flow control may have more data in the network than it can effectively handle, so that data is delayed (often beyond usefulness) and throughput may actually decrease as the demand increases.

In a crisis situation, it can be safely assumed that the traffic input to the network will rise to and surpass any available communication capacity. Thus flow control will be necessary to allow the most important data to pass through the network, and to provide a fair sharing of the network resources among the system users.

An added requirement in the tactical environment is protecting the network from being flooded by inputs from a captured terminal. Effective flow control will have the added benefit of limiting the potency of this threat.

Any implementation of flow control involves the process of measuring the level of traffic in the network, exchanging this information (in some form) among the nodes of the network, and throttling the access of data entering the network.

The current approaches to flow control can be divided into the general methods of *buffer limits*, *end-to-end windows*, *choke-packets*, and *backpressure*.

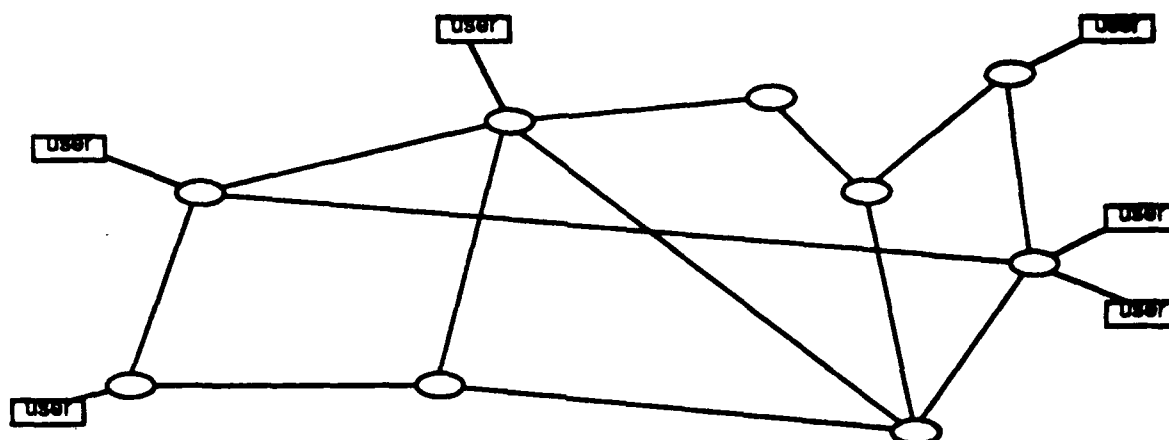


Figure 15. A Mesh Architecture

1.4.3.5. Point-to-Point Channels

Point-to-point channels are the basis for traditional long-haul systems. Data are forwarded over an interconnected mesh of channels, as illustrated in Figure 15. For completeness, however, three reasonable multi-hop architectures based on point-to-point channels are mentioned.

1.4.3.5.1. Store-and-Forward Mesh

The store-and-forward mesh has served as the basis for almost all long-haul packet-switched communication. It allows efficient use of long-haul channels, even for bursty data, by providing fairly sophisticated switching components for connecting them.

One of the advantages of the mesh is that it offers an arbitrary redundancy, while sharing the redundant channels among a large number of users. The result of this is a highly cost-effective survivability.

Methods for topology design considering survivability are fairly well established^{14,15}, although the theoretical issue of optimal topology design still retains some open questions.

The problem of logical link control has been solved for standard network implementations. It can be implemented cheaply and effectively while using a negligible portion of the channel capacity.

The only attack on logical links that has been identified is the selective jamming of certain packets in a sequence, for example every eighth packet in a window of size eight. Whether an adversary would consider this a feasible attack is unclear, as the

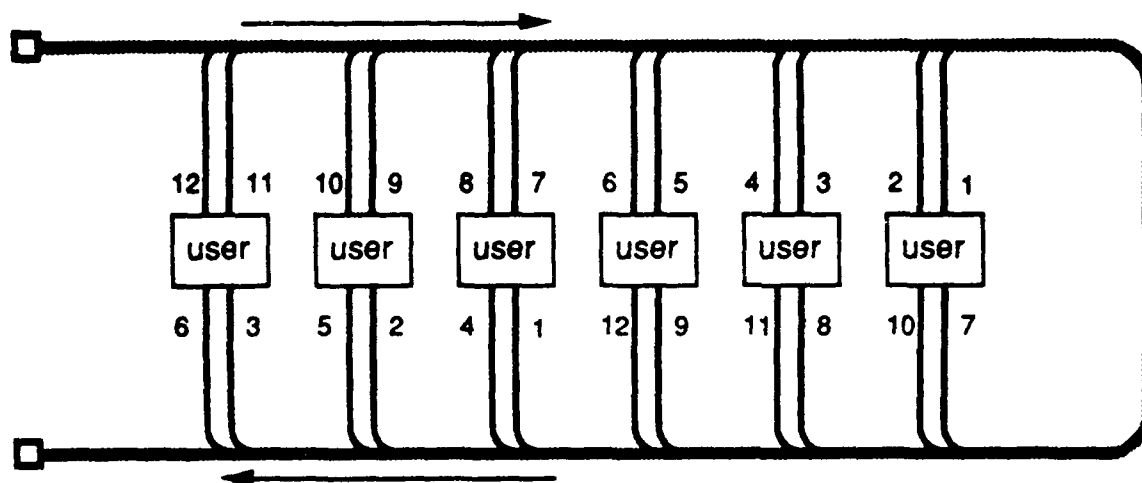


Figure 16. An Interconnection Topology

threat is minor compared to attacks on the physical layer, media access layer, or network layer that would have much greater effectiveness while requiring no more in terms of hardware.

Changes may be made in the logical link to better take advantage of changing technologies, such as the integration of a variety of traffic types, fast forwarding, and behavior in packet radio networks, but these may be easily solved. The best option for the most part will be to track current technology and adjust logical link behavior to conform to the standards of the time.

1.4.3.5.2. Interconnection Networks

Several alternatives based on constraining the structure of the mesh are possible, with the intention of providing simpler switching structure¹⁶. Simplicity in the switching structure will become increasingly attractive in many situations due to the ease of implementation with photonic switching devices.

One example of such an architecture is that proposed by Karol and Hyluchj which uses wavelength-division multiplexing on a single optical channel, with each user operating with two input ports and two output ports, as illustrated in Figure 16. The numbers in the figure indicate channels. It is easily confirmed that a simple routing structure exists so that any user may send data to other users within a few hops.

A similar architecture is also possible with multiple fibers as well as wavelengths, adding to the survivability of such a system.

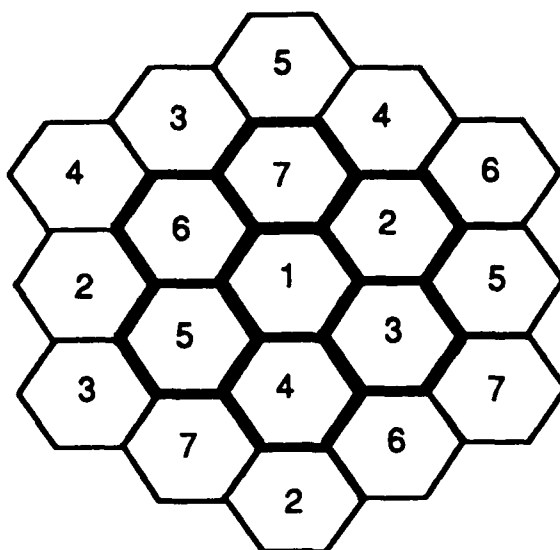


Figure 17: Seven Cell Frequency Reuse Pattern

1.4.3.5.3. Cellular Radio

Cellular mobile radio is based on the spatial distribution of frequencies in a repeating cellular pattern. For example, suppose that the set of available frequencies is divided up into subsets labeled 1 through 7. These subsets are assigned in the cellular pattern shown below in Figure 17. The pattern is designed to maximize frequency reuse geographically while keeping units assigned to the same frequency maximally separated to reduce interference.

In most applications there is a fixed control hub at the center of each cell. The hubs are tied to the long-haul network as well as each other to allow mobile units to communicate with whomever they wish. As mobile units move through the cells, they are handed off from one hub to another, ensuring that there will be no loss of contact.

In sophisticated cellular schemes the frequency assignments can be dynamically reallocated to account for varying demand throughout the network. This would be an important capability in a tactical environment. Unfortunately the hubs present an excellent target for enemy bombardment. Redundancy and adaptive transmitter power levels must be employed to improve survivability.

1.4.3.6. Broadcast Channels

Current visions of multi-hop networks using broadcast channels fall into two categories, depending on whether the users can be easily divided into self-contained groups that share each broadcast medium. If this is the case, then access to each medium is similar to that for a single hop broadcast system, and the broadcasts can be said to be non-overlapping. If each user has its own set of "neighbors" to which it can broadcast, but on channels shared by other users, sometimes beyond the range of the first user, then the broadcasts can be said to be partially overlapping. These will be considered in separate sections.

1.4.3.6.1. Partially Overlapping Broadcasts

The current application of Partially Overlapping Broadcasts is in Packet Radio Networks. In Packet Radio Networks packets are broadcast only to a number of radios geographically near the transmitting radio. An example of the architecture is shown in Figure 18. Packets typically are delivered to a destination via store-and-forward routing through a series of nodes. The adaptability to mobile subscribers and versatile and survivable implementation make packet radio an excellent candidate for tactical communications. Some sort of multiple-access method is required for packet radio access, and the techniques may depend highly on the type and nature of the available frequency spectrum.

Leiner, Nielson, and Tobagi¹⁷ discuss three design areas specifically connected to Packet Radio Networks, these are:

- radio connectivity and channel sharing, dealing with the choice of channels and media access
- link management and routing, dealing with network layer issues
- user interfaces

For this discussion, a finer subdivision of these is appropriate.

1.4.3.6.1.1. Connectivity

To the degree possible, a connection must be maintained among all pairs of users. For the maintenance of connectivity, the following issues must be addressed in design:

- what frequency band to operate in

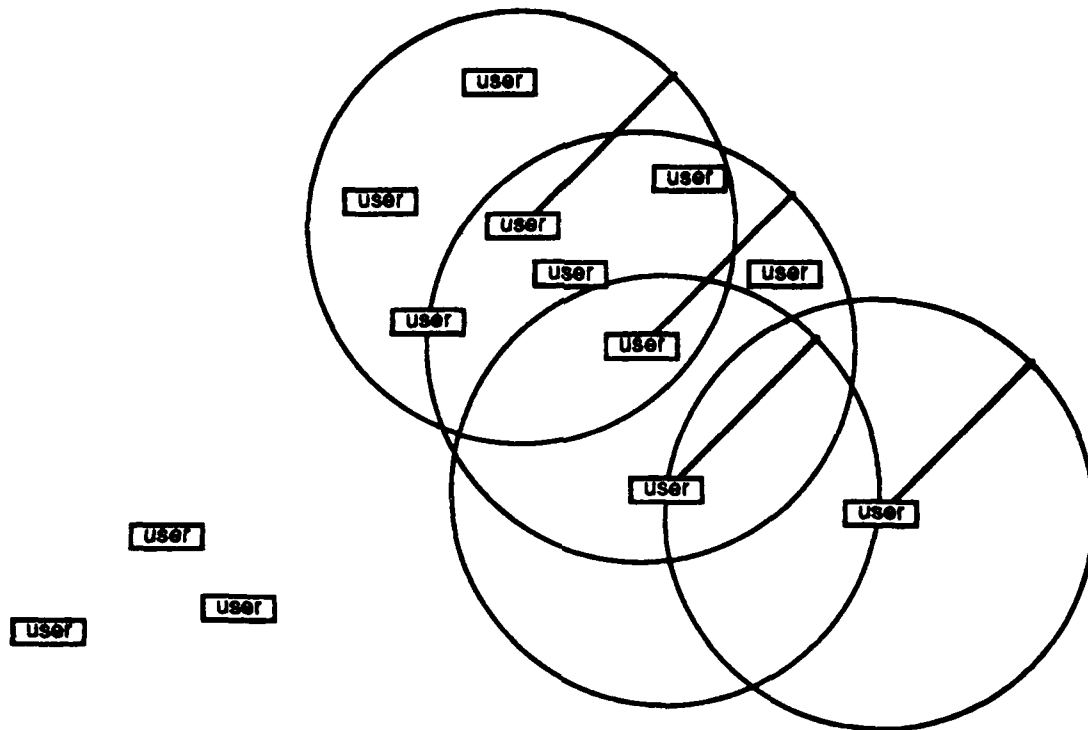


Figure 18. A Network with Partially Overlapping Broadcasts

- how much bandwidth is required
- how the bandwidth is allocated in time and space

These three topics are closely coupled. The frequency band strongly affects the radius of transmission and therefore the topology of the network. If a lower frequency is used, the frequency band can be quite significant, since it will strongly affect the radius of transmission and therefore the topology of the network.

The amount of bandwidth required depends on several factors, and is coupled to the network topology and hence the problem of what frequency band to use. The factors are:

- how much data must be sent through the network
- how many hops are required to reach a destination (depends on topology)
- how much overhead information is required (depends on topology and frequency of topology changes)

- to what degree may bandwidth be divided in space, i.e., reused at other geographic locations (depends on frequency band and transmitter power)
- what is the efficiency of channel use (depends on channel access method and coding/encryption techniques)

1.4.3.6.1.2. Channel Access

There are three basic themes that arise with channel access. They correspond directly to access on any bus system:

- deterministic division of the channel in time, frequency, or code assignment (TDMA, FDMA, CDMA)
- random access with some type of collision resolution
- reservation schemes

Random access schemes can be subdivided into those that use carrier sensing and those that do not. Accurate performance analysis has not yet been completed, but it appears that schemes using carrier sensing can have much worse performance than simpler schemes that do not. This is because the sensing may actually provide misinformation due to the propagation delays in the system (accentuated when higher data rates are used) and also the existence of "hidden nodes" which are outside the range of a node, but close enough to interfere with the receiving end of a transmission.

A deterministic division of channels has the classical problem of being rather inefficient for bursty users, which can be expected on the tactical battlefield. On the more positive side, it also provides a very natural method of sharing a channel fairly among several users.

Reservation schemes may provide an excellent compromise between these systems, although it requires some knowledge of expected traffic and a significant amount of overhead in maintaining the reservation links. Investigations of reservation schemes have not yet appeared in the research literature.

Note that techniques involving control passing (for example, token passing or polling) are not appropriate here, since the relatively uncoordinated overlapping of broadcasts makes the proper maintenance of a logical ring very difficult.

Each of these schemes allows for the introduction of spread-spectrum techniques. Code division of packets adds to the value of carrier

sensing, at the cost of greatly increased complexity. Coding of preambles may also help in the process of access. It is important that coding does not interfere with the ability of all nodes to hear all neighbors, at least with some codes.

Another alternative in coding is for the preamble of a packet to contain information regarding the spreading waveform used, so that the receiver can program its matched filter accordingly.

1.4.3.6.1.3. Link management

The link between two nodes can be much more complex with packet radio networks than with other systems, since the behavior of each link can be highly unreliable and time varying. ARQ and FEC schemes will probably have to be combined in a dynamic manner for the system to be used effectively.

Related to this is the issue of how link layer acknowledgements should be implemented. Explicit short acknowledgements are possible, but may essentially double the number of packets in the system. An alternative is for the transmitting link to wait to hear the subsequent link transmit the packet again, thus providing a passive acknowledgement. The latter scheme seems to lower the channel use, but requires the acknowledgement scheme to be able to handle much longer delays before the acknowledgement of a packet, since these passive acknowledgements can no longer be given priority in the system.

Current opinion seems to favor explicit short acknowledgements.

There is also an opinion that hop-by-hop acknowledgements should be forgone altogether, and that acknowledgements should be left to the source and destination. The counter to this is that individual channels are unreliable enough that such a structure would greatly increase inefficiency.

Unmentioned is the method of having each node periodically sending a larger "acknowledgement packet" to all of its neighbors, perhaps in conjunction with other connectivity information. This larger packet would provide a compromise between the earlier packets by acknowledging several packets at a time, but still providing time limits on the time for acknowledgement.

Finally, the link layer must constantly update the existence of links. The main problem is to be responsive to changing topology while avoiding very short lived outages which may occur with subscribers that are mobile while transmitting. An issue is whether this is best

accomplished by retaining special hardware to measure channels, or by basing the connectivity decision on the link layer information itself.

1.4.3.6.1.4. Routing

How should routes be established and maintained? This question can be broken into the two issues of

- how should routing information be disseminated?
- how should the routing information be used?

Three basic methods have been identified:

- flooding, where no attempt is made to store routes
- point-to-point methods, where a route or set of routes is associated with each source-destination pair
- connectionless methods, where some information about topology and destinations is maintained, but individual connections are not set up.

Flooding is simple but inefficient. Packets are replicated a large number of times before reaching a destination. On the other hand, little or no routing information must be maintained.

Point-to-point methods, while efficient for stable topologies, is not necessarily effective when the topology is changing rapidly, since each change in topology requires the reestablishment of several links.

Connectionless methods allow routes to be updated without relying on individual connections. With these methods, each node makes routing decisions on the basis of the node from which a packet came, and its destination address.

It should be noted that routing in packet radio networks differs from routing in conventional networks in two respects:

- rather than a routing decision of "which link do I send this on," each node makes decisions of "do I retransmit this packet."

- replication of packets can be expected as a regular occurrence.

The dissemination of routing information is perhaps the most critical portion of routing design. The use of a central location is impractical for the tactical environment, so the routing mechanism must operate in a distributed manner.

A portion of this routing problem is what information should be tacked onto passing packets, versus information that is disseminated in explicit packets.

Although the problem of routing is still poorly understood, a few results have been obtained¹⁸.

1.4.3.6.1.5. Flow Control

It is desirable in any network that shares channels for traffic to be limited at the entry to the network so that congestion is controlled. This problem is still not well understood with "classical" packet-switched networks, and becomes much more complex with packet radio networks. While the development of effective flow control may strongly influence other aspects of network design, it is unfortunate that the only suggestion that can be provided at the present time is that considerable research is needed in this area.

1.4.3.6.1.6. Deployment and Maintenance

The operation of a packet radio network requires initial deployment of the system, and maintenance to retain connectivity. The deployment must be made to provide an adequately connected system. The degree of connectivity depends on the distance between users, the frequency range used, the power used, etc. In a tactical environment, the system must be adjustable to satisfy a variety of configurations. Therefore the system should respond adaptively to deployment. The exception is that additional "repeater" nodes may be needed in some situations. It appears that the easiest way to do this is by having an adjustable transmitter power.

A question that must be answered with regard to this is what transmission range is most desirable. Some preliminary analysis suggests the following as reasonable criteria¹⁹:

- if all nodes have the same transmission range, the maximum capacity is reached when the average *nodal degree*—the number of other nodes with which a node can communicate—is 15 to 25 (with networks of 60 nodes using CDMA)
- if the transmission range of each node is adjusted to allow it to reach the same number of neighbors the maximum capacity is reached when the average nodal degree is around 11.

Thus transmitter power could be adjusted so that each user can reach approximately 11 other users.

Of course, any good design will include a full complement of startup diagnostics for the network.

When the topology changes due to nodes that are destroyed or move out of range, then some maintenance must be performed. The network should remain fully operational at all other nodes when this happens. An unresolved issue is whether notification should be sent someplace when the topology changes.

The capability for remote diagnostics and maintenance, while probably quite valuable, may not be as necessary for packet radio networks as for some other environments, since a nonfunctioning piece of equipment can presumably be easily moved to a troubleshooting location.

1.4.3.6.2. Non-Overlapping Broadcasts

In a system of non-overlapping broadcast channels, packets must be forwarded through bridges that connect the individual broadcast systems, as illustrated in Figure 19. A full discussion of these systems is difficult, since a theoretical understanding these systems has not yet been developed.

One implementation of such a system is SURVNET, designed by MITRE as a survivable network in a base level environment²⁰. This system uses a fiber-optic bus using a token passing access protocol. Several users are dual homed to the bus in physically separate locations. If the bus becomes partitioned, the segments self-reorganize into smaller separate bus systems, and the dual-homed users are capable of acting as bridges between the partitioned systems. From the economic standpoint, a major cost of this system is probably the cost of nodes that must serve effectively as bridges in the event of multiple faults.

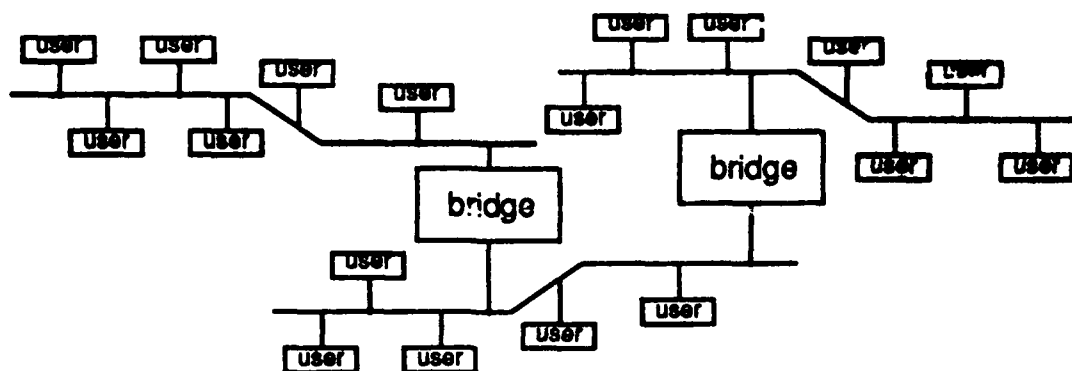


Figure 19. A Network with Non-Overlapping Broadcasts

1.4.3.7. Hybrid Architectures

An additional option that must be mentioned is a hybrid system combining two or more of the above architectures. Due to the additional overhead of managing multiple architectural needs, such architectures should be avoided unless there is an overriding justification for the combination of architectures in a single system, and the additional cost of effective implementation is marginal.

1.5. Internetworking Options

1.5.1. Gateways

1.5.1.1. Gateways for Packet Radio Networks

Gateways may be called upon to serve the additional role of providing connectivity when a network becomes partitioned. The mobile nature of subscribers creates an additional addressing problem. When a network is partitioned, does it represent two separate networks to a gateway, or a single network. If it represents two networks, the gateway must know whether or not it is partitioned. If it represents one network, the gateway must be certain of which partition a packet must be forwarded on. Connectivity enhancement by connection through other networks should be possible.

1.6. Higher Layer Options

The transport layer should not cause significant problems, now or later. Current analysis indicates that even with current technology, correctly implemented transport protocols are capable of handling data at rates of several hundred Mbps. Thus little or no updating of transport layer protocols will be necessary, at least from the performance standpoint²¹.

A full investigation of higher layers is beyond the scope of this report, but there is one higher layer issue that reflects directly on the network layer and lower layers. This is the problem of captured terminals.

One very important problem is the wide host accessibility once network access has been gained. Therefore access points on the network should be considered a weak point in protecting networks from unwanted host entry²².

2. Requirements and the Suitability of Options for Non-Mobile Subscribers

2.1. Requirements

2.1.1. NATO Requirements

NATO documentation²³ presents the following requirements for the Post-2000 era:

- **formal messages.** This implies a requirement for reliable transfer and acknowledgement.
- **radio silence.** This implies a capability for highly reliable communication without acknowledgements. It is assumed that radio silence will be important only on broadcast channels. This would be most important for over-the-horizon channels, but also may arise for high-frequency channels during some operations.
- **mobile command posts.** The command posts are expected to be smaller and more mobile, and consist of a number of relatively self-contained cells which can operate in a wide variety of configurations. Interconnections within and between collocated cells are expected to be via high-data-rate LANs. Emissive communications will be severely curtailed. This adds the requirement that groups added to or "visiting" a mobile command post may have to rely on command post communication systems.

The last requirement points to two special communication needs:

- a quickly deployable local area network to connect the self-contained cells.
- a quickly deployable nonemissive mechanism for connecting a mobile command post to lower and higher echelons.

The latter need is by far the more difficult to implement from a technical standpoint.

NATO suggests that the rapid growth of cellular radio for public telephone use may be matched by increased use in the military environment.

NATO documentation disclaims responsibility for implementation of components within an HQ, which is held to be a national responsibility, rather than directly a NATO one.

2.1.2. US Army Requirements

The Army's tactical communication requirements for the post-2000 land combat zone are a function of perceived force deployment patterns and anticipated threat. The deployment pattern determines the required connectivity. There will be a variety of mobile and non-mobile forces arranged in a hierarchical fashion. Local forces will be connected in a Local Area Network (LAN). The LANs will be connected to a larger network which is in turn part of a long-haul network that ties the FLOT to the rear of the sustaining area.

The anticipated threat determines what sort of survivability must be included within this concentric set of networks. The post-2000 tactical theater can best be characterized as extremely fast-paced and extremely lethal²⁴. Tactical communication systems must be capable of fast relocation and reconfiguration. They must also be able to handle sudden heavy bursts of message traffic while maintaining an acceptable throughput level.

The development of anti-radiation weaponry (e.g. HARM missile) will lead to severe restrictions on emissive communication equipment. Equipment with salient electromagnetic signatures can expect to enjoy extremely brief operational lifetimes. Message traffic switching points are the most susceptible to attack.

The sophistication and power level of jammers will continue to increase. A corresponding emphasis must be placed on spread spectrum techniques and confined channels such as fiber optics and copper wire.

Finally the most important requirement is that the communication mission continue to be performed despite the destruction of a large percentage of the hardware assets. This capability is obtained through the inclusion of various types of redundancy.

2.1.3. US Air Force Requirements

The Air Force's operational requirements will be reviewed by first discussing the current state of development of Air Force communication capability. Next the Air Force's view of 21st Century Command and Control will be described. Finally the Air Force's current understanding of 21st Century communication requirements will be discussed.

2.1.3.1. Current Air Force Communication Outlook

Meetings with Air Force personnel produced the conclusions that their main current concern is communication between air bases. The current operational requirements, which they expect to remain constant over the next several decades, is for communication among²⁵

- a relatively small number of air bases located far behind the FLOT with massive communication needs
- a larger number of sensors that must communicate with one or more air bases. These installations may be mobile or non-mobile, and will typically be located in friendly territory. The Air Force expects that the sensors will be netted together for survivable connectivity as well as integration of data.
- aircraft, air defense sites, etc. These will be discussed under Mobile Subscriber Requirements.

The primary operational requirement seen by Air Force personnel is the maintenance of connectivity between air bases to the point of annihilation of the air base. This has driven the Air Force to be primarily concerned with interconnecting a wide variety of media to ensure the reliability of connections.

The Air Force's field of vision for current development plans extends approximately seven years²⁶.

The Air Force plans to handle communication with aircraft through the JTIDS program, which will be discussed under mobile communications.

2.3.1.2. The Air Force's Tactical C² Environment

The Air Force's Command and Control requirements include the variables of threat, geography, command structure, mission objective, political/diplomatic sensitivities, climatic environment, joint/combined force structure, and duration.

Also affecting the future requirements is the following observation by the Air Force:

Advanced Technology is rapidly altering the character of the air war in terms of weapon system speed and lethality and also by giving tactical commanders the capability to see further and more clearly into the adversary's rear area.

The Air Force's view of communications requirements for the 21st Century are (a more complete list can be found in the document, 21st Century Tactical Command and Control Architecture, Table II.1):

- survivability (held to be key)
- the ability to support cycle-time reductions of 5:1; The daily air tasking and fragmentary orders generation process must be shortened from the current 24-30 hours to a maximum of 6-7 hours.
- dependability even in degraded modes
- modularity
- flexibility
- transportability²⁷.

The Air Force stipulates a requirement for rapid exchange of intelligence and operations information across national and allied security boundaries.

The architectural nature of the the Air Force's C² System combines the components of physical dispersion, replicated data bases, and distributed functions.

The Air Force has divided its tactical C² functions into the areas of Air Surveillance Management and Control (ASMC), Surface Surveillance Management and Control (SSMC), and Force Planning (FP). These functions are well-summarized in the document, 21st

Century Tactical Command and Control Architecture, in Figures II-1, II-2, and II-3.

Underlying all of these architectures are access elements that may perform any of a variety of tasks. These elements will appear as special purpose devices to their operators, but may be reassigned to other tasks as circumstances dictate.

For the ASMC architecture, the Air Force requires the capability to dynamically reallocate geographical areas of responsibility, a fully distributed data base, and *complete information exchange*. They expect information transfer to be initiated by the source in a broadcast format. Data must be updated every few seconds and transmitted without request throughout the area of operations. This is currently accommodated by JTIDS.

For the SSMC architecture, it is expected that each node will have a highly specific data base of information, and that each node will procedurally request only that information relevant to its specific assigned functions. In the area of SSMC, the stipulation is added that sensors must be sufficiently flexible to support a concentrated effort in an objective area while providing continuous coverage of other areas with little or no mission degradation. That is, a sensor must be able to "zoom in" on a particular area of interest. Also, the integration of data from multiple sensors is required to enhance overall system performance, flexibility, responsiveness, and survivability. This will include on-board target correlation and deconfliction, classification, identification, data compression. All of these will drive the architectural characteristics of a standardized interface, selective collection and processing of data, and design to facilitate satisfying human decision processes.

The FP architecture will coordinate a very large data base on enemy order of battle, enemy strengths and weaknesses, detailed information on enemy objectives and likely targets, locations of enemy threat units, friendly force status, availability, weapon/aircraft and aircrew capabilities and limitations. It is expected that this database will be distributed, and that both broadcast and query formats will be heavily used. Dispersion of planning elements and redundancy is intended to ensure survivability at each level in the Command Structure.

The Air Force recognizes a need to interact with other services and such support services as logistics, weather, personnel, security, civil engineering, comptroller, public affairs, chaplain, and safety.

The Air Force sees a need for Local Area Networks for communication in a small area.

The Air Force envisions modularity at two levels, which they call the shelter module and the workstation module. The relative roles of modularity at these levels do not seem to be entirely resolved.

The Air Force also requires that components be able to support a wide variety of functions, with the specific application of an equipment dependent on the person using it.

2.3.1.3. The Air Force's View of the Communications Environment

On the basis of these requirements, The Air Force envisions communications systems that must be survivable, secure, jam-resistant, and "common user."

The Air Force sees the principal areas for research and development in communication networks as

- relays (it is not clear what is meant by this; apparently it refers to packet-radio network nodes)
- precedence
- security
- multi-media management and control.

The Air Force sees its communication architecture as characterized by a high rate of communication within each "subarchitecture" (ASMC, SSMC, FP), and a much lower rate of communication between these subarchitectures and with other entities.

The Air Force estimates that C² nodes in a local area will communicate with each other with data rates up to 500 Mbps.

The communication over greater areas is conceived to be carried out with (apparently) something like LOS packet radio at rates up to 100 Mbps. RF communications here are assumed to be omnidirectional, "although certain special routes may be directional." It is not clear what the expected geographical extent of such a network is. The documentation indicates that this is for communication "within a subarchitecture" although this would not represent a reasonable communication architecture.

The communication between subarchitectures is conceived to be done by an ISDN network involving a variety of media.

The network protocols address both single- and multiple-destination communication, with capabilities for priority, precedence, and preemption.

For all situations, survivability is emphasized:

In essence, the [Communication System] must not contribute to the disruption, deception, destruction, or exploitation [by the enemy] of the C² system.

The survivability is to be obtained via alternate routing, relays, and common signaling.

The Air Force also requires their systems to be topology-independent and have a building-block approach.

The Air Force requires interoperability not only among communication links, but among data models, machine processes, and operating systems.

The Air Force sees the following tasks that must be done in the development of a communication system:

- establish message sets, formats, and protocols to support efficient inter-/intra-net throughput yet be compatible with standard interfaces.
- incorporate network security for sensitive multi-source data, to include provisions for multi-national operation
- integrate voice and data switching and a network management capability.

The Air Force states that the communication system should have:

- a demonstrated capability to dynamically and simultaneously allocate media
- features to stringently control types and sizes of messages
- the capability to provide efficient flow control from input to output
- backward compatibility features
- ease of maintenance features
- embedded cryptography

- the capability to operate in any environment
- a transition plan for evolutionary implementation

2.1.4. Navy Requirements

The Navy lists a number of requirements for communication systems, with survivability emphasized.

Current Navy Requirements call for a fiber optic ring system for base communications, based on the IEEE 802.5 Token Ring.

Other plans call for the development of cabling and connection systems to the dock for direct communication with docked ships²⁸.

According to Navy documentation, most tactical conversations are made up of only two voice transmissions, and most of the remaining conversations are made up of eight or fewer voice transmissions lasting up to fifteen seconds. Almost all tactical conversations last less than one and a half minutes²⁹.

2.1.5. Defense Communication Agency Requirements

The Defense Communication Agency (DCA) has developed requirements for long-haul sustaining base communications and end-user needs. Their main concern is reducing cost and staffing while maintaining services, and improving functionality, survivability, and security³⁰.

The DMS requirements are drawn from the draft *Multicommand Required Operational Capability K-38*. They are:

- **Connectivity/Interoperability.** All users should be able to communicate with each other and with systems of U. S. Allies, other government agencies, and defence contractors. Furthermore, messages should be delivered as close to the reader as possible.
- **Guaranteed Delivery.** Messages must be delivered with a high degree of assurance, and accountability must be present.
- **Timely Delivery.** There must be a capability for priorities, and a means of dynamically adjusting to changing traffic loads.

- **Confidentiality/Security.** All classified and other sensitive message traffic must be protected, and released only to authorized recipients.
- **Sender Authentication.** The receiver of a message must be able to verify the source.
- **Integrity.** The information content of messages must not be changed.
- **Survivability.** The services must be as survivable as the users they serve.
- **Availability/Reliability.** Services should be available to users on a continuous basis.
- **Ease of Use.** Services should allow user operation without extensive training.
- **Identification of Recipients.** Each sender must be able to designate the recipient of each message unambiguously.
- **Preparation Support.** User friendly preparation of messages must be available.
- **Storage and Retrieval Support.** A capability must exist for messages to be stored for a period of time after delivery. This should include readdressal, retransmission, and automated message handling functions such as archiving and analysis with a capability for incorporation into future messages.
- **Distribution Determination and Delivery.** The system must deliver messages within the requirements of the recipient organization, and must deliver them to the individuals specified by the originator.

Many of these requirements relate more to standards than to system architectures, and will be drawn upon further when standards issues are addressed.

DCA sees the current AUTODIN and DDN architectures as evolving to a much more efficient and effective system to be achieved by FY 2008. They hold that the major thrust of the change is a shift towards standardization and interoperability. The primary components of the change are:

- The current DDN will be replaced by a communication subnet (Defense Communication System) designed to

provide custom tailored communications capabilities to users (voice, data, facsimile, video, etc.). This will be accompanied by an integrated set of common-user services.

- At the base level, the 4KHz analog voice systems will be replaced by a large bandwidth Installation Information Transfer Systems (IITS). This will be an ISDN-based capability fully interoperable with the wide area system.

2.2. Suitability of Options

The above requirements indicate that non-mobile subscribers are generally well behind the FLOT and often organized into reasonably large bases. This structure suggests three categories of communication systems that must be considered:

- long-haul communications, for communication among bases sensors, and connection points to mobile subscribers
- base level communication, for communication within a base
- local area communication, for communication within a small building or a section of a large building
- host systems, for interfacing with a host.

These echelons are similar, but not identical, to echelons that arise naturally in civilian systems. The precise nature of each of these categories of communication and the suitability of options for each will be described in the sections below.

Connection to the larger system generally will fall to the smaller system. This is the only practical approach, since to do otherwise would be to place a burden of connecting to what may be a very large variety of smaller systems on the large system. To the degree possible, the smaller system should appear as a single user to the larger system.

2.2.1. Long-Haul Communication

Long-haul communications is for all communications from or to a base or other non-mobile subscriber. It does not include communications within a base. Long-haul communications has the following characteristics:

- the geographical distance covered by a link may be arbitrarily long
- all long-haul channels must be assumed to be non-secure
- the long-haul channels are by far the most costly component of the system, and any additional complexity that provides a non-negligible improvement in the efficiency of channel use is likely to be justified.

2.2.1.1. Physical Channel Options

The selection of a primary medium for long-haul communications is a study in conflicting goals. The expense involved in manufacturing and deploying long-haul equipment places a heavy emphasis on maximizing data rate while minimizing overhead and delay. On the other hand the geographic extent of the long-haul channel makes it extremely vulnerable to both passive and active interception as well as sabotage. This is particularly true in rear areas where personnel may not be carefully monitored and an unfamiliar face may not be cause for alarm. If the long-haul medium is designed as a single highly efficient trunk line, the impact of destruction through sabotage or bombardment becomes enormous.

The solution lies in the combination of two concepts developed earlier in the section on media options. Fiber optical cable is suggested as the primary medium. The availability of practically unlimited bandwidth allows for the multiplexing of a large number of signals on a single trunk. The relative permanence of the long-haul channel reduces the deployment problems associated with confined channels. Survivability is provided through spatial redundancy and the establishment of secondary and tertiary media. Repeater stations can be used to minimize delay due to repair and to maximize the probability of detecting and locating passive and active interceptors.

The secondary and tertiary media should be selected from among the atmospheric/free space options. Factors contributing to the destruction of a fiber optical link will have a similarly deleterious effect on wire, wave guide, or any other confined channel media. Given the distances involved, OTH HF and VHF links are suggested for the secondary medium. SHF/EHF satellite links are an acceptable third alternative.

In all of the media options discussed above encryption must be used to secure information transmitted over the channels. This not only

ensures privacy, but minimizes the risk of an active interceptor placing false information on the channel.

2.2.1.2. Networking Options

NATO believes budgetary constraints will require a move towards public network type WAN's, including transition towards an ISDN type system³¹. It is our opinion that this assessment is correct.

As the number of reasonable alternatives is small, and the number of explicit and implicit requirements is quite large, the networking options will be discussed individually, with pertinent factors regarding the suitability of each included.

Reasonable candidate options for Long-haul communication include:

- single repeater systems
- one point-to-point mesh
- several point-to-point meshes

These will be discussed in turn, including a description of the pertinent factors regarding the suitability of each.

2.2.1.2.1. A Single-Repeater Broadcast System

Such a system would presumably depend on the use of a Geosynchronous satellite.

This system would provide quickly transportable links, and a flexible adjustment of footprint, but would potentially be limited in capacity and provide only very limited survivability.

2.2.1.2.2. One Point-to-Point Mesh

The long-haul communication requirements provide a classic example of where a mesh of point-to-point channels is most appropriate. The physical dispersion of the channels can accommodate arbitrary requirements for survivability and bandwidth.

The topology, especially when leaving a base, must depend on multiple physical media. Confined channels must be diversified both in terms of origination on the base, and in physical paths by which they leave the base.

2.2.1.2.3. Several Point-to-Point Meshes

One issue which remains unclear is whether long-haul networks will evolve to one large system, or to several smaller systems that are interconnected. The interconnection of multiple networks adds significant overhead and delay to the communication process, but the political and administrative demand for separate structures is likely to continue into the far term. Thus we should expect, especially in the NATO environment, that interconnection of multiple systems will be part of the communication system.

An interconnected group of several meshes retains all of the issues inherent with a single point-to-point mesh, plus additional issues of how to route and control flow through multiple networks.

2.2.1.3. Higher-Level Options

The establishment of higher-level options can be expected to be a complex one, since a number of individual systems, political attitudes, and language barriers must be accommodated. How these issues are best addressed is still an open problem. The best approach to these problems is to begin the process of negotiating a common set of protocols that will meet these needs.

Protocols for the Transport Layer may have little need to evolve from current standards. The Application Layer, where common applications for the military environment, should receive early attention.

It has been the attitude of current standards groups that the Presentation Layer is becoming less important, as many systems have become more compatible. For the NATO environment, the Presentation Layer may again become important in at least being able to provide a very limited set of commands and responses in a variety of languages.

2.2.2. Base Level Systems

2.2.2.1. Physical Channel Options

The sabotage and interception threats in the physical layers of the long-haul and base level communication links are comparable. The fundamental difference between the two lies in the extent of the geographic region involved. Fiber optical cable remains the best choice for the primary medium. The secondary media should be

changed, however, to take advantage of the reduced distances. Line of sight communications should be emphasized, ranging from UHF through EHF and optical frequencies.

2.2.2.2. Networking Options

Candidate options include:

- Individual point-to-point systems
- General mesh type architectures
- Single-hop directional propagation systems
- Double ring architectures
- A number of local area networks interconnected by gateways
- Constrained meshes with highly modular nodes.

2.2.2.2.1. Individual point-to-point connections

As each new system is implemented on a base, the administrators of this system might desire a single point-to-point connection to handle its communication needs. While this may seem to be simpler from the administrative viewpoint, the disadvantages discussed in Chapter 1 will far outweigh these considerations from the viewpoint of the entire base. Therefore this option is presented mainly to point out its unsuitability. The lack of suitability is due to:

- the overall increase in administrative and deployment costs
- poor survivability
- lack of flexibility and connectivity.

Avoiding an expensive and ineffective conglomeration of individual connections requires the foresight to install a flexible, easily accessible base system that is capable of handling all requirements.

2.2.2.2.2. General Mesh Architectures

The use of general mesh architectures, with relatively expensive switches designed for the efficient utilization of long-haul channels, is not likely to present a cost-effective solution to base-level networking. It is reasonable to expect that a system that is not quite

as efficient in the use of channels, but is much less costly, will prove to be a better alternative.

Two arguments in favor of a general mesh are:

- the base-level system could be implemented purely as a part of the long-haul network, although with much higher data rates
- with the continued expansion of computing technology, switching for this type of network may be only marginally more expensive than other implementations.

While the first point may provide a theoretically more efficient system, it is expected that administrative concerns will drive the need for separate systems (i.e., a base-level system dedicated to communications on the base), even at the cost of some efficiency. The second argument is probably not as valid, as the much higher data rates expected on a base can be expected to be operating at the limits of technology, so that the implementation of the more complex system will continue to be more costly.

2.2.2.2.3. Single-Hop Directional Propagation Systems

This is an option which is expected to be strongly considered for commercial systems. It is not suitable for a military environment, because of its poor survivability. A single hit will nullify these systems.

2.2.2.2.4. Rings

Similarly, rings also suffer from very poor survivability, and will not be suitable for the military environment in the far term.

It should be noted that this statement is contrary to current Navy thinking, where a fiber optic ring system is planned for future base-level communications. Their plans call for addressing the problem of survivability by laying cable underground, so that it will remain fairly impervious to attack.

It is our opinion that while this may be considered an adequate approach for the next one or even two decades, the lack of inherent survivability in the architecture, even with a subterranean installation, will make the system ineffective in the very far term tactical environment.

2.2.2.2.5. Double Rings

This has already proven to be a strong candidate in the commercial world for implementation as a Metropolitan Area Network.

The double ring has a much greater survivability than the single ring discussed in the previous section. This is due to the ability to loopback from one channel to the other when a break in the channel occurs. Thus connectivity is maintained in the face of a single hit, and even after multiple hits it is possible for segments of the system to act as separate single rings.

Another argument in favor of the double ring is its advanced state of current development, so that even within a few years of this report it will become generally considered as an established technology.

In spite of these advantages, the survivability of double rings remains inherently limited. The operation of the system as several smaller rings in the presence of multiple failures does not fully comply with the operational requirement for connectivity and the strong emphasis on survivability.

Thus while the possibility of the double ring should be retained as a low-cost option with established technology, it is our opinion that it does not meet the stated far-term requirements.

2.2.2.2.6. Interconnected LANs

One architecture that may be used is to have several local area networks interconnected by gateways. This would provide a natural evolution from separate local area networks implemented on a base. By a high degree of interconnection, an arbitrary survivability could be implemented.

The performance of this type of system is not yet well understood, and remains an open research problem. Furthermore, utilizing a sequence of local area systems for base level communication may interfere with the traffic in some local area systems, and would produce an awkward administrative structure. Finally, as discussed elsewhere in this report, it is expected that the implementation of local area networks is best done on an individual basis according to the needs of a specific administrative unit, and such an architecture coordinates poorly with this plan.

On the basis of these concerns, an interconnection of local area networks will not provide an effective base-level system.

2.2.2.2.7. Constrained Meshes

There are several means of constraining the classical mesh architecture to provide simple and effective communications on the base level.

One option is the implementation of a particular topology of interconnections. The use of such schemes allows implementation of much simpler routing, even in the face of node failures, and the implementation of less expensive nodes. The cost is that more connections may be necessary, or some packets may be lost in transmission, but these effects are much less important on a base level than in a long-haul system. Most of these schemes are built around a node with a limited number of connections.

One option which depends on full duplex channels is a Spiral type architecture³². This allows "self-routing," simple expandability, and high survivability in case of failure.

Another approach designed specifically for optical fiber networks has been investigated by Karol and Hyluchj. An expansion of this type of architecture is a highly likely candidate for base-level communications.

2.2.2.3. Internetworking with Long-Haul Communication Systems

This must be done via gateways. The gateway must be accessible to all users on a base, so that the base-level system can fulfil its proper role as a connector to the long-haul network. The long-haul network must view the gateway as a single user in its system.

2.2.3. Local Area Systems

It is expected that local area systems will arise in a variety of formats for different functions, and a wide range of possibilities may be used. In spite of this, certain structures should be considered as standard, at least for common applications.

2.2.3.1. Physical Channel Options

The limited area covered by a local area system has a large impact on the design of the lower layers of the tactical communication system. Sabotage and interception are not a serious threat and need not be factored into the design equation. Survivability is also not a major factor because of the limited gradient between a complete miss and the total destruction of the equipment. As a result the need

for secondary media is questionable. The principal design criteria lie with the avoidance of jamming and destruction through enemy attack. Other criterion include transportability and ease of operation. The authors concur with current NATO documentation in predicting that LANs will become increasingly dependent on fiber optic technology³³. Fiber optical cable limits electromagnetic emissions, minimizing detectability as well as susceptibility to jamming. The reduced transmission power levels allow for the design of lighter equipment that is more easily carried by men in the field.

2.2.3.2. Networking Options

Candidate options for local area networks include:

- bus
- ring
- point-to-point
- double ring
- directional channel
- as a subportion of a base-level network.

The suitability of busses, rings, and point-to-point channels can be gleaned directly from the general discussion of them in Chapter 1. In short, busses are flexible in implementation and operational characteristics, but not particularly survivable and limited in the possible data rates achievable; rings are less survivable than busses; and point-to-point channels are notoriously unsurvivable, inefficient, and ultimately costly.

Double rings show improvements in survivability over these systems at the cost of additional complexity. The current implementation of double rings in a Metropolitan Area environment demonstrates the viability of such systems when a high data rate is required.

Directional channels have a number of long-term advantages:

- no constraints on diameter from a performance standpoint
- the size can be determined from administrative and survivability factors
- theoretically arbitrary data rates

- ease of implementation of fiber optic channels.

Several specific implementations on directional channels are possible. Again, a variety of options might be present.

If interconnection networks for base-level communications becomes inexpensive, another option for communication is for an area previously considered "local" to be treated as a specific subportion of the larger base network. An additional consideration here is that most single-hop networks are not particularly survivable, and a single "hit" on the channel may end communication for the network (this is not as true with fiber optical channels). Thus the use of local area networks may be reduced to smaller administrative blocks, with a more survivable base level system for communicating among the blocks. This will also allow simpler, cheaper communication systems for the individual LANs (for example, CHEAPERNET).

2.2.3.3. Internetworking with Base Level and Long-Haul Communication Systems

Local systems should be capable of interfacing with a base-level system. Connection to the long-haul system should be achieved through the base-level system.

2.2.3.4. Higher-Level Options

Higher-level options for a local area network are highly application dependent. Any administrative unit should plan to use a single communication network for all communication needs.

3. Requirements and the Suitability of Options for Mobile Subscribers

One feature of future communication systems is that the transmission capacities of non-mobile and mobile communications can be expected to differ by several orders of magnitude. The fundamental limitations imposed by mobile communication will make the communications much smaller in available bandwidth, and much greater in cost. Mobile communications will necessarily have to rely on atmospheric propagation, with corresponding limitations on bandwidth and complex requirements for repeating stations. Thus the communication to, from, and among mobile units will be of a much more restricted nature than among non-mobile units, so that in relative terms, the types of information passed on mobile channels must be chosen and processed with much greater circumspection.

Operational planning should include a significant decrease in the level of information transfer to and from mobile subscribers. For example, while video signals may become commonplace within non-mobile communication, the integration of video signals into mobile communication systems will have a much more limited application.

A consequence of this is that, subject to operational constraints, efficient utilization of bandwidth can be expected to be the ultimate driver in mobile communication systems.

3.1. Requirements

3.1.1. Air Force Requirements

The Air Force's mobile operational requirements are primarily concerned with communication with aircraft. Communication with missiles should also be expected as a concern in the future. A requirement also exists for communication between aircraft and ground air-defense systems.

The Air Force does not seem to have developed communication requirements for aircraft in the far term. Presumably, aircraft will continue to perform the same tactical missions that they have performed in the past. These missions include surveillance and monitoring, support of ground forces, destruction of enemy assets in

their sustaining base, and protection of other aircraft. Two recently developed missions have been the use of aircraft as command posts and as communication relays. The Air Force's mission in the tactical arena will thus involve flights over friendly as well as enemy territory. It is expected that flights over enemy territory will be at either treetop altitudes (ground attack missions by stealth aircraft) or extremely high altitudes (surveillance, monitoring, and communication relays for forward forces). Flights at intermediate altitudes will be far too dangerous for most purposes due to the improvements in radar and laser guided weaponry. Aircraft over friendly and enemy territory will each have different communication needs. Forward low-flying aircraft will require airborne relays over friendly territory or satellite relays. High flying aircraft can use long range LOS communication links.

The current technology for tactical communication with aircraft is the JTIDS (Joint Tactical Information Distribution System) Program, which is designed for information distribution, position location, and identification capabilities for tactical forces.

3.1.2. Army Requirements

The principal difference between the Army's non-mobile and mobile communication requirements is the obvious requirement that the physical and higher level media allow for changes in the geographic distribution of nodes. Radio and free space optical links will thus form a dominant element in network design for mobile land forces. It is anticipated, however, that some units shall be more actively mobile than others. "Mobile" units that remain stationary for long periods of time may benefit from the use of seemingly inappropriate media such as fiber optical cable.

3.2. Suitability of Options

The above requirements indicate the following general categories of mobile communication needs:

- mobile command posts at each level of command up to the Corp Echelon, with internal and external communication
- mobile communication over the length and depth of the front
- interfaces to non-mobile communication systems

- communication devices carried by ground mobile vehicles that serve a particular tactical function (tanks, artillery, etc.)
- mobile sensors
- communication devices carried by personnel on foot
- aircraft.

As with non-mobile users, the communication needs can be divided into ranges of scale as:

- long-haul mobile communication
- mobile connections over a medium-range geographical area, such as that covered by a corp, division, or brigade
- communications within a local area such as a command post, a mobile vehicle, a mobile sensor or platoon.

In addition to these, there are two systems with requirements special enough to warrant separate consideration. These are:

- mobile command posts
- aircraft.

Finally there are two important connection problems, which will also be treated separately:

- connection from mobile communications to a long-haul non-mobile network
- connection from a local area to the mobile network.

3.2.1. Long-Range Mobile Communication

In this section, we consider the requirement for communication among mobile units separated by an arbitrary geographical distance. The requirement for such communication is generally on a lower scale than other mobile communication requirements, but a complete communication system should provide this capability.

Two options are possible:

- satellite communication
- connection via a long-haul non-mobile network

The effectiveness of satellite communication is difficult to predict, given the uncertain long-term efficacy of satellites for tactical communication.

As mobile units, especially those that have long-range communication requirements, can be expected to be well connected to medium-range networks, and through them to a long-haul non-mobile networks, utilizing the long-haul non-mobile network as the long-range connector is a very sensible alternative. The connection should then be more secure and more reliable, and would require no additional equipment for this need.

3.2.2. Medium-Range Mobile Communication

There is a strong requirement for communication among a large number of ground-based mobile units distributed over the range of territory covered by one or several corps. Before this can be properly addressed, it is useful to divide the users of this system into three categories:

- highly mobile ground-based units, which move frequently and require full communication capability while moving
- relocatable ground-based units, which may move frequently but for which communication only takes place in a stationary mode, and may involve some set-up and teardown. This may include mobile sensors, repeaters for a medium-range communication system, and Mobile command posts as discussed below.
- deployable ground-based units, which can be expected to move only infrequently during a tactical encounter, but which require rapid deployment during or just prior to a tactical encounter. An example of this may be a corp command post, some mobile sensors, and some repeaters for mobile communication connectivity well behind the FLOT.

There are two fundamental alternatives that must be considered for these systems:

- packet radio networks
- cellular radio networks

On the basis of the discussion of these, we will also consider the alternative of a hybrid system combining elements of both.

3.2.2.1. Packet Radio Networks

Packet radio networks operate on the basis of partially overlapping broadcasts. Access to a channel is by contention. Because of this, each user can be aware of all other users within its broadcast range, so that the local topology can be constantly monitored and updated, even with a rapidly changing topology. These factors provide very simple deployment and relatively simple reconfiguration.

The current literature has heavily emphasized packet radio systems for mobile tactical communications, based on the ease of rapid reconfiguration as nodes are lost. However, many intractable design problems remain to be solved before the packet radio networks will provide effective channel utilization.

Most of the issues that must be resolved are discussed in Section 1.4.3.6.1. In short, at the current level of development, the channel utilization is low, the efficiency of the system is further reduced by the inefficiency of the routing algorithms, and to our knowledge the problem of flow control has not even been addressed.

These factors align poorly with the concept that the scarce resource in these systems will be bandwidth, so that its poor use is a significant negative factor associated with packet radio networks.

3.2.2.2. Cellular Radio Networks

Cellular radio networks are based on a mesh topology and use frequency and or code assignment on atmospheric channels.

Because of their fairly structured architecture, the deployment of cellular radio systems can be rigid, with significant effort required for determining the proper assignments of channels for a situation. Furthermore, when some channels are lost, the reestablishment of channels can be difficult and awkward, since a user may be in contact with only a few other users in its vicinity. These shortcomings can be partially overcome by the use of hot-standbys, but this can lead to significant extra expense. For these reasons,

cellular radio systems have not been viewed favorably for far-term mobile communications.

Once channels are assigned, cellular radio networks can be very efficient in channel usage. Since channels are assigned to pairs of users, their utilization can be quite high. Furthermore, conventional mechanisms for routing and flow control can be implemented.

3.2.2.3. Hybrid Networks

The similarity of the physical channel structure of packet radio networks and cellular radio networks, combined with their highly contrasting advantages and disadvantages, strongly suggests the consideration of a hybrid architecture combining the advantages of both.

More precisely, a mobile cellular system, with explicit channel assignments, would be used for the communication of all data on the network. A very limited numbers of channels would be set aside for the maintenance of the network configuration. These channels would act in a contention mode and would allow near neighbors to exchange topology and channel assignment information. On the basis of this, channel assignments could be updated according circumstance in a rapid, distributed manner.

The additional cost of such an implementation over a purely packet radio network or purely cellular network would be marginal.

Thus it is our opinion that such a system is highly suitable for the mobile communication environment.

3.2.3. Local Area Mobile Communications

Local area mobile communication among ground based units requires an easily deployable local area network. The implementation in a local area further implies that the main expense will be access devices, so that simple architectures must be implemented.

A variety of options are available for this situation, including systems based on confined channels, systems based on local broadcast, and directed low-power LOS radio communications. Because of the variety of applications, each of these may be most suitable in some situations.

Architectures based on confined channels must be easily deployed and repaired, and must overcome the poor survivability inherent in these systems. This will require easily replaced, modular

components. Since confined channels must be deployed before use, such a system will not be usable while a ground unit is mobile, and will require at least a minimal setup and teardown time.

Systems based on local broadcast will permit use while moving, but may suffer from interference with other local area systems and disruption by the enemy. The system will be highly survivable and can remain in operation as long as there are users to communicate.

Directed low-power LOS communications must also be deployed before use. These systems will be more survivable than systems with confined channels, and less disruptible than local broadcast systems, but also suffer partially from the problems of both. The transmissions should have a tight beamwidth to minimize detectability and further reduce transmitted power levels.

An issue with all of these is whether commercially developed technologies will be applicable for this environment. It can be expected that commercial LAN systems are not likely to be directly applied to the tactical mobile environment, so that at least some modification of commercial systems must be undertaken.

3.2.4. Connection from Mobile Systems to a Long-Haul Non-Mobile Network

Since there will be fundamentally different parameters in the design of a mobile network and a non-mobile long-haul network, it must be assumed that they will operate as separate systems, and that communication between them must be accomplished by gateways.

Since the point of connection of the gateway may not be well known, the responsibility should lie with the non-mobile network to provide appropriate connection points for attachment of a gateway. Responsibility for the gateway and mobile communication to the gateway should lie with the mobile system.

Connectivity to the non-mobile system may require communication over a long distance through friendly or hostile territory. The options for this connection include:

- a direct connection from the medium-range mobile network
- an over-the-horizon communication channel
- satellite connections
- commandeered public communications media.

Each of these options will be discussed in turn.

3.2.4.1. Local Connection

A local connection can be achieved when the long-haul non-mobile network extends to within a close proximity of the mobile network. Over near enough distances, additional repeaters can be used to extend the range of the mobile network.

This approach becomes impractical when the distance from the mobile network to the long-haul network becomes too great.

3.2.4.2. Over-the-Horizon Radio

An over-the-horizon radio with much greater range than the mobile network can be used to cover longer distances. This approach is practical when the distance is too great for a more direct connection, the demand for bandwidth is sufficiently small to avoid making the connection a communications bottleneck, and the connection is sufficiently removed from the FLOT so that it is not particularly sensitive to electronic countermeasures.

3.2.4.3. Satellite Channels

Satellites provide a great range for connection, and are capable of providing sufficient bandwidth for all conceivable demand.

As with other applications, the potential use of satellites for tactical communications in the far term is diminished by the unpredictable level of survivability of such systems.

Although light conflict in remote locations is not directly covered by this report, it should be pointed out that satellites are an excellent alternative for connection from a mobile network to a long-haul mobile network in such a situation.

3.2.4.4. Commandeered Public Communication Channels

In the time frame covered by this report, it is reasonable to expect that Europe will have developed and implemented a very high bandwidth fiber optic network extending to almost all parts of the continent.

In this environment local connection to the public network and connection through it to the non-mobile long-haul network provides an excellent connection alternative, and can provide high

bandwidth to a far greater range of locations than could be expected to be achieved by a purely military network.

This approach can also be quite effective for deployable mobile units which will not expect frequent moves.

In order for this method to be effective, compatibility with public communication systems must be maintained.

The political ramifications of this alternative are beyond the scope of this report.

3.2.5. Connection from Local Area Mobile Systems to Medium-Range Mobile Systems

The connection between local systems and the medium-range mobile network must be accomplished by a gateway collocated with the local system. The gateway will appear as an ordinary node to the medium-range mobile network.

3.2.6. Communication to and from the Mobile Command Post

The mobile command post, with its very stringent requirements on mobility, nondeductibility, and communication within the post, represents a special communication problem for the future tactical battlefield.

Due to the conflicting requirements on non-emissive communications, and mobile communications to all other echelons, the only viable option for the mobile command post is for it to be made to look like an ordinary node in the medium-range mobile communication system.

It should be emphasized that this requires that the mobile command post not be viewed as a central hub. It may also require the placement of additional repeaters in geographical locations typically associated with command posts.

3.2.7. Communication within the Mobile Command Post

The mobile command post is envisioned to be a collection of vehicles deployed in a distributed fashion on the battlefield. This is motivated by the need to increase the survivability of the system and to separate the emissive (and therefore easily targeted) component from the remainder of the command post. Each distinct

component is to be self-contained and useful in a variety of configurations with a variety of other units. Data rate requirements for communication among these units are anticipated to be high.

The selection of a primary medium ultimately rests on a tradeoff between the level of mobility, the imperviance to interference, and the data rate.

If the command post, once located in a given position, is expected to remain for a significant period of time, then a multiply connected fiber optic system is in order. The primary benefit of this approach is the available bandwidth and the immunity to detection. The negative attributes include slower set-up time and vulnerability to disruption by armored vehicles and enemy fire. Secondary media should include one or more forms of LOS radio.

If the command post is to be moved too frequently for the use of fiber optical cable, then LOS radio should be adopted as the primary medium. The principal benefits include easy set-up, while the disadvantages include sensitivity to weather and terrain. These disadvantages are offset partially by the ability to locate units of the command post nearer each other in poor weather or rough terrain.

While the complementary benefits of the two options might suggest pursuit of both, this approach is not fully satisfactory. The requirement for implementation in a wide variety of formats constrains all units to be interoperable with all others, so that units with different types of connections will not ultimately provide an effective solution.

Thus one of the options should be selected for standard use. Since the other system will be the only option in some situations (either the high bandwidth of the optical connection or the high mobility of the LOS radio), the option not chosen for standard use must be available as an added module for those special purposes.

Implementation of both options on all units will add unnecessarily to the weight and cost of the mobile units.

Which of the two options is preferred must await a more precise specification of requirements.

3.2.8. Aircraft Communication

3.2.8.1. Long-Range Communication

Clearly an atmospheric channel must be used for communication with aircraft. This leaves two options:

- broadcast systems
- directed beam systems.

Broadcast systems provide a relatively simple implementation, but can achieve only an extremely limited throughput, so that applications beyond very short messages or positioning information cannot be anticipated.

Directed beam systems represent a technological challenge, especially with the implementation of light directional antennae on aircraft. Thus implementation from ground to air may be much simpler than implementation from air to ground.

Another problem is that aircraft in enemy territory can be expected to be flying at a very low altitude, so that directional communication may still not be possible, except from aircraft flying at a high altitude in friendly territory.

The U.S. Air Force has not specified a requirement for high-rate communication with aircraft. If such a requirement is developed in the future, directional beams (electromagnetic or optical) will comprise the only reasonable option.

3.2.8.2. Communication within an Airborne Formation

Radio communication using center frequencies around 60 GHz is an interesting option for close-in communication between aircraft. Detectability and jammability is severely curtailed when communication is conducted near the resonant frequencies of oxygen or water molecules. The main technological hurdle in this area is the difficulty in developing EHF omnidirectional antennae.

4. Recommendation of a Message Switching Architecture for the Post 2000 Tactical Communications System

The message switching architecture for the Post-2000 tactical environment is driven by the following factors:

- projected user requirements
- projected limits of communication technology
- projected cost-effectiveness.

The communication architecture must satisfy all user requirements. Since the system must handle effectively a wide variety of operational requirements, the architecture must match each the operational requirements as needed by a separate architecture, and to interconnect these by gateways.

Gateways are currently regarded by many as a necessary evil, adding great expense and interfering with performance. While some of the major problems can be expected to be resolved, gateways may still be a bottleneck in the communication process in the far term. Nevertheless, an interconnection of several systems via gateways allows the architecture to be driven directly by user needs, which is the proper priority. The alternative is to design a more costly system that fails to meet user needs.

The limits of communication technology have been fully discussed in Chapter 1. Certain limitations can be placed on the ability to satisfy user requirements well into the future, such as the much lower data rates and increased complexity with mobile communication when compared to non-mobile communication.

When several reasonable alternatives arise for the satisfaction of a communication requirement, a judgement must be made on which will prove to be the most cost-effective. While estimated cost figures for the time-frame covered in this report would be meaningless, informed judgements can be made by considering which components of a system are expected to be the most expensive or scarce, and optimizing the use of those components.

The subsystems and interconnection of the recommended architecture is illustrated in Figure 20. Each of the subsystems will be discussed individually.

4.1. Non-Mobile Long-Haul Communications

Non-mobile long-haul communications should be carried out through a highly connected network. This system will provide a very high rate of data almost entirely composed of fiber optical channels. Other media may also be used, and can serve as a backup to the fiber optical system, but should consist primarily of previously existing channels.

Whether the non-mobile communications will consist of one large network or several several smaller networks should be driven by political considerations rather than technical ones. From the technical standpoint, one large network is preferred, but interconnection of several smaller networks is also feasible.

The long-haul system should correspond as closely as possible to commercial standards. The one feature which can be expected to deviate from standard commercial networks is that a high degree of connectivity will be necessary to ensure survivability. This should not interfere significantly with the remainder of the architecture.

4.2. Non-Mobile Base-Level Communications

On the basis of the above considerations, the best system for base-level communications appears to be a constrained mesh of optical fibers interconnected by photonic switching devices.

The devices should be of a uniform and standard design. To allow flexibility of interconnections, the switching device should provide, in addition to a local input and output connections, a small, standardized number (two, three, or four) of input and output connections to other switching devices.

The topology of the interconnecting lines must be managed to enable high connectivity on physically separate paths, including relative assurance of return paths. This will be balanced by requirements for low cost, which can be achieved with wavelength-division multiplexing on single fibers.

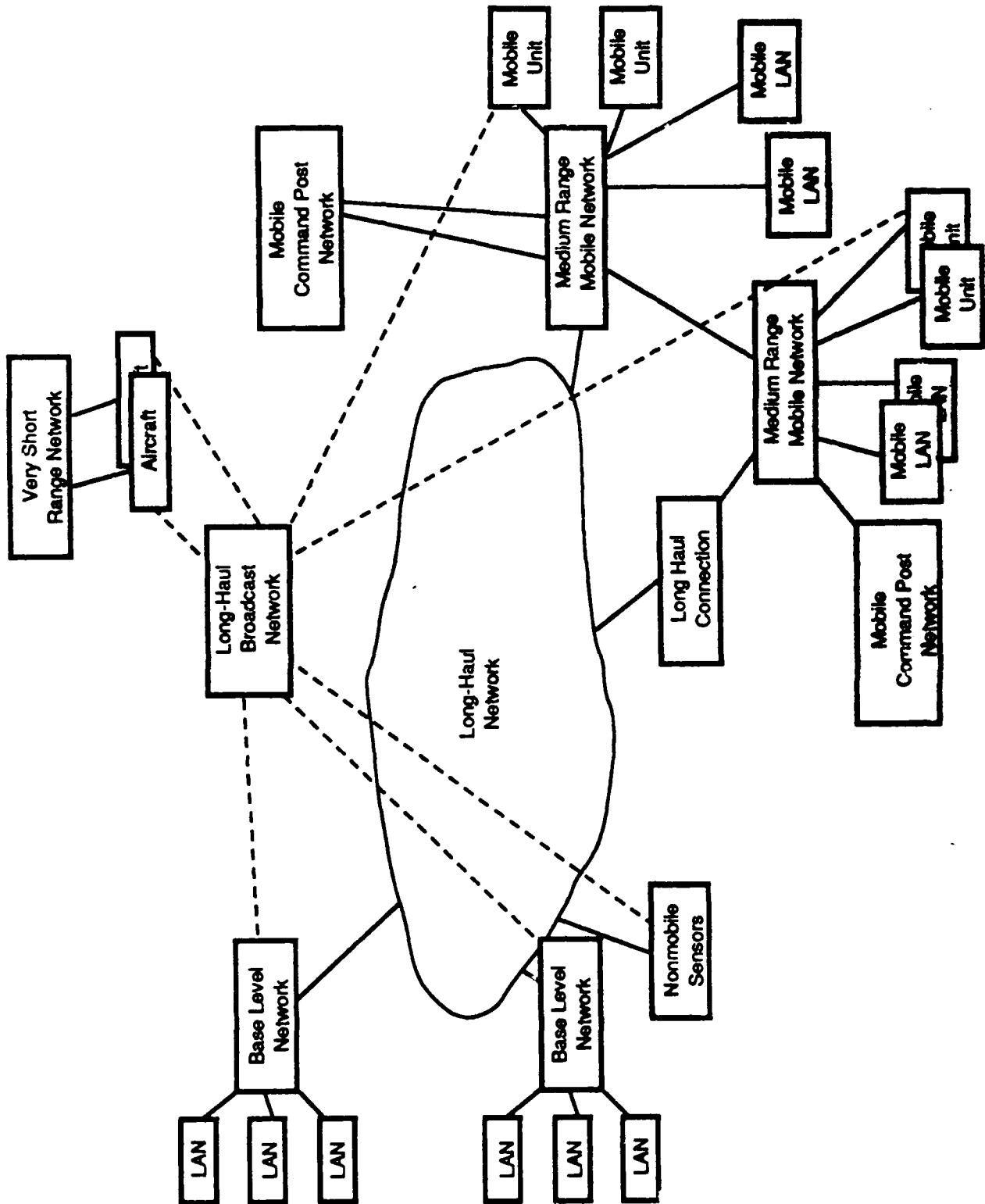


Figure 20. The Proposed Architecture.

The best size, specific updating procedures, etc. have not yet been determined by the research community. Most research on such interconnection systems have so far have dealt only with very simple topologies.

There is one note of caution that must be included with this recommendation. Although photonic switching is very promising, the state of development at the time of this report has not yet demonstrated the existence of a fully viable switching technology. If, in fact, photonic switching does not turn out to be a viable alternative, the envisioned system will prove meaningless.

4.3. Non-Mobile Local Area Communications

The implementation of Local Area Networks in non-mobile environments is expected to be driven by administrative concerns. Thus LANs will be implemented within well-defined administrative boundaries.

The architectural requirements on Local Area Networks will not differ significantly from those of commercial networks. Therefore the expectation should be for commercially available networking technology, or modifications of the same (such as TEMPESTing), to be fully usable in the military environment. Considerable leeway should be allowed in a unit's choice of LAN architecture. The choice should take into account individual concerns and commercial trends.

With the development and implementation of base-level systems, LANs will be implemented in areas of a much smaller size than that allowed by current implementations (i.e., within a room or a wing of a building, as opposed to through an entire building or between buildings). A LAN will be an appropriate alternative when the following conditions are met:

- there is a well-defined administrative unit requiring significant internal communication, or one where it is cost-effective to provide a LAN for gateway access to the base-level system
- it is acceptable for a single hit during a tactical encounter to bring down the network.

While it is unlikely that a local area architecture will prove viable for the base in the long term, the possibility does exist that local area networks may be superseded by direct connections onto the base-

level system. This would depend on the equipment costs for the base-level system becoming low enough for this alternative to be viable, and on an administrative desire for such a connection. In the end, the local topology can be expected to be driven by administrative convenience, for which local area networks with a gateway connection to the base-level network may be retained in spite of greater cost and lower system efficiency .

4.4. Ground-Based Mobile Medium-Range Communication

Ground-based mobile medium-range communication should be implemented as a hybrid system consisting of a distributed cellular network of atmospheric channels tracked and maintained through subchannels acting in a packet-radio mode.

The current state of research leaves such systems poorly understood. In particular, the problem of topology maintenance and channel assignment is not well understood. Furthermore, routing and flow control may be complicated by the ability to dynamically reconfigure the network for more efficient operation.

However, a few features of the system can be specified. In particular, the implementation of adjustable transmitter power and the use of spread-spectrum techniques have proven to be very effective in similar architectures.

4.5. Ground-Based Mobile Local Area Communication

Local area communication systems must be available for a variety of mobile applications. To meet these applications, all of the options discussed in Chapter 3 should be pursued. The architecture should match those of commercial systems as closely as possible, with appropriate modifications to allow use in the mobile environment.

4.6. Communication for the Mobile Command Post

The mobile command post should appear as an ordinary node in the mobile medium-range network. Due to the special features of locations chosen for command posts, repeaters in the mobile medium-range network should be placed in locations typically chosen for command posts.

Connection from within the command post to the medium-range network node should be through the command post's internal communication system.

The main issue in communication among the units of a mobile command post is the media. At this point two alternatives should be pursued: fiber optic interconnection and LOS radio. Once requirements for the degree of mobility and the data rate are fully specified, one of these options should be selected to be implemented on all mobile units, with the other available as an add-on feature for special operations.

4.7. Airborne Communication

The special features of communication with aircraft will continue to require a special communication mechanism.

The low throughput broadcast mechanism such as is currently implemented using the JTIDS system will remain a vital portion of aircraft communication. The only respect in which improvement over the current system can be expected is greater attention to performance issues, including throughput and the response to congestion. Otherwise the JTIDS architecture can be expected to remain stable over the next several decades.

There has been no specification of communication with aircraft beyond that provided by the JTIDS system. Some alternatives for additional communication may be considered, however.

Highly directional antennae from the ground may provide additional LOS communication with ground locations. The current view is that such systems would be prohibitively complex, especially for implementation on aircraft. Thus if such systems come into existence, it could be expected that communication from ground to aircraft will far precede communication in the return direction.

If breakthroughs occur in the implementation of EHF omnidirectional antennae, radio communication among aircraft using center frequencies around the resonant frequencies of oxygen or water should be implemented for communication within an airborne formation.

5. Standards for the Land Combat Zone

Since most non-mobile communication concerns share most of their features with civilian systems, integration and correspondence with civilian standards is strongly recommended.

5.1. An Approach to Development of Standards for the Post-2000 Tactical Environment

There are a few underlying principles that must be laid before a full discussion of standards can be developed:

- The development of standards is partially technical and partially political.
- For the far term, the recommendation of specific implementations of standards is not very productive.
- It will be very much in the interest of NATO to conform as closely as possible to commercial standards in every circumstance possible.

One of the consequences of this is that one of the prime issues in the discussion of standards is whether commercial standards will be developed in conjunction with a particular element of the architecture. If such a commercial standard is expected to be available, the best NATO reaction is to plan to adopt the commercial standard. In the formation of the standard, NATO should ensure that the few special features of particular interest to a military environment are addressed in the specification process. For portions of the architecture for which commercial standards are not expected to be available, explicit efforts must be undertaken to develop appropriate standards for the future systems.

For the standards that must be developed, it has been established in the standards process that careful timing is essential to the effectiveness of a standard. If a standard is developed before the ramifications of alternative design features are fully understood by the research community, the effectiveness of the system is likely to fall far short of its potential. If a standard is developed after production of a system is underway, the standard is likely to be ignored or inconsistently applied. Thus the development of the standard must fall in the gap between these two events.

A dilemma arises if the gap is too short, so that there is no effective time period for the standard to be developed. The best way to avoid this problem is to promote examination of the issues by the research community well in advance of any expected deployment.

5.2. Physical, Media Access, and Network Layer Standards

5.2.1. Non-Mobile Communication Standards

5.2.1.1. Non-Mobile Local Area Communications

In accordance with the above architectural recommendations, NATO should allow the implementation of standards for local area networks for non-mobile applications to be fully developed and driven by commercial concerns. Modifications required for military applications (such as TEMPESTing) should not effect the implementation or development of standards.

Standards for the interface between local area networks and base level networks must await the development of standards for base-level communication.

5.2.1.2. Base-Level Communications

As these systems can be expected to be developed with a fundamentally different architecture than commercial systems, the utilization of commercial standards can be expected to be minimal.

One exception to this may be utilization of existing standards for the physical layer, including specifications of cabling and physical interfaces.

Current Navy requirements call for a fiber optic ring system for base communications, based on the IEEE 802.5 Token Ring. This must be viewed as a short-term solution to the base-level communication problem.

Standards for the interface between base-level communications and long-haul networks must await the development of standards for base-level communication.

5.2.1.3. Non-Mobile Long-Haul Communications

The current indication is that military long-haul communication systems will closely match systems developed by commercial

industry, with the exception of implementation with higher connectivity. Therefore NATO should plan to utilize commercial standards, and should participate in the development of the standards in the role of an interested potential user.

Physical layer standards are expected to deal with optical fiber issues.

Logical Link standards may change little in their basic structure from current designs, with the exception that much higher data rates will result in much larger window sizes.

The development of effective routing and flow control mechanisms for these system currently in the very beginnings of research. As the understanding of these systems improves, standards will need to be established.

5.2.1.4. Interfacing among Long-Haul Non-Mobile Networks

This should be developed in conjunction with commercial standards.

Issues of particular interest to NATO will be the development of visa standards for the transfer of data across international boundaries, and standards for the implementation of multi-level security.

5.2.2. Mobile Communication Standards

5.3.1. Connection from Long-Haul Non-Mobile Networks to Medium-Range Mobile Networks

As this application is of interest only to the military, NATO should plan to spearhead the development of all standards needed for these systems.

Until the fundamental architectures for these systems are better understood, standards for them should not be developed. Therefore a wait of several years from the publication of this report should occur before the standardization process begins.

5.3.2. Medium-Range Mobile Networks

As the military has the prime interest in systems of this type, NATO should also plan to spearhead the development of standards for these systems. There may be some interaction with civilian standards however, in that mobile communications has and will become a commercially viable industry. In particular, NATO must

ensure an adequate assignment of frequency spectra to satisfy its mobile communication requirements.

The theoretical understanding of the architectures associated with medium-range mobile networks is still in its infancy. Attempts to establish standards for these systems will be most effective if delayed five to ten years from the time of this report, when the behavior of these systems should be much better understood.

5.3.3. Interface from Medium-Range to Mobile Local Area Networks

Standards for this interface must be developed concurrently with the development of medium-range systems. Until the nature of medium-range mobile networks and mobile LANs is better understood, the interface cannot be precisely prescribed.

5.3.4. Mobile Local Area Networks

The degree to which standards will need to be developed for mobile LANs will depend on the degree to which they differ from conventional Local Area Networks. At the very least, standards for interconnection of modular components at the physical layer will need to be developed independently by the military. The need for development of standards at the Media Access, Link, and Network layers will depend on the specific implementation used.

5.3.5. Communications within a Mobile Command Post

The environment of the mobile command post will remain entirely one of interest only to the military. Therefore the military should plan to develop standards for all parts of communication between units as part of the development of mobile command post systems.

5.3.6. Aircraft Communications

As this report recommends continuation of the current broadcast system for aircraft communication, little or no modification of current standards are expected. The only exception is that improvements may be made to the efficiency of channel sharing, for which corresponding standards will need to be developed.

Narrowbeam communication to and from aircraft remains an unexplored area. If and when such systems are implemented, standards will need to be designed accordingly.

Similarly, standards for communication among aircraft will need to be developed in coordination with the determination of need. The standards may be expected to correspond closely to current local area broadcast access methods.

5.3. Higher-Layer Standards

There are a variety of sets of standards currently embraced by various organizations. In particular, DCA is embracing the X.400/X.500/SDNS protocols for user services³⁴. The Navy has shown great interest in the GOSIP suite of protocols, etc.

It is expected that in the far term, methods of developing and specifying protocols will far exceed current methods. As the possibility arises, a set of higher layer standards suitable for transfer of all types of data from all applications across all networks should be established to the fullest extent possible.

As most higher-layer functionality for military applications will closely match the functionality for commercial applications, NATO should develop standards for the higher layers in conjunction with commercial elements, and ensure any specific features (such as those mentioned in Section 2.1.5., for example) required in the military environment are maintained.

¹J. F. Brouwer, "Half a Century of 'Electronification' in Telephony Systems," *Phillips Tech. Rev.*, Vol. 42, No. 10/11/12, September 1986, pp. 361-373.

²R. W. Lucky, "The Gigabit Network: Who Needs It?," *IEEE Spectrum*, Vol. 26, No. 9, September 1989, p. 8.

³As documented in the *U.S. Army AirLand Battle Plan (Heavy)*.

⁴This negative aspect can be turned into a positive one. Short range atmospheric EHF communications are extremely hard to intercept without placing the intercepting antenna directly between the friendly transmitter and receiver. See "Prototype Tests Secure Millimeter Communications" by Paul Steffes and Ronald Meck, *Microwave Systems News*, October, 1980, pp. 59-68.

⁵—, "Background to ATCCIS Communications," NATO ATCCIS Working Paper 34A.

⁶Meeting with Air Force Personnel in Rome, NY, May 18, 1989.

⁷Military historians feel that an intercepted message led the usually cautious George McClellan to force Robert E. Lee into an early encounter at Antietam, preventing him from completing the positioning of his forces.

⁸The security of a cryptosystem should not rely on the design of the system itself (polyphonic substitution, Vigenere, etc.) but on the particular key used by the system to encrypt messages. The key is an input to the cryptographic system that is changed regularly. The cryptosystem itself need not be changed at all.

⁹W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, Volume IT-22, Number 6, November 1976, pp. 644-654.

¹⁰—, "Background to ATCCIS Communications," NATO ATCCIS Working Paper 34A.

¹¹R. P. Kosowsky, I. M. Jacobs, and K. S. Gilhousen, "ARNS: A New Link Layer Protocol," *Proceedings of the 1988 International Conference on Communications*, pp. 26.5.1-26.5.5.

¹²A. Bhargava, J. F. Kurose, and D. Towsley, "A Hybrid Media Access Protocol for High-Speed Ring Networks," *IEEE JSAC*, Vol. 6, No. 6, July 1988, pp. 924-933.

¹³A. Ephremides and S. Verdu, "Control and Optimization Methods in Communication Network Problems," *IEEE Transactions on Automatic Control*, Vol. AC-34, No. 9, September 1989, pp. 930-942.

¹⁴K. T. Newport and M. A. Schroeder, "Network Survivability Through Connectivity Optimization," *Proceedings of the 1987 International Conference on Communications*, Vol. 1, June 1987, pp. 471-477.

¹⁵M. A. Schroeder and K. T. Newport, "Augmenting Tactical Communications Networks to Enhance Survivability," *Proceedings of the 1988 International Conference on Communications*, pp. 26.4.1-26.4.7.

¹⁶Several proposed methods are discussed in *IEEE JSAC*, Vol. 6, No. 6, July 1988.

-
- 17 Barry M. Leiner, Donald L. Nielson, and Fouad A. Tobagi, "Issues in Packet Radio Network Design," *Proceedings of the IEEE*, Vol. 75, No. 1, January 1987, pp. 6-20.
- 18 V. O. K. Li and R.-F. Chang, "Proposed Routing Algorithms for the U. S. Army Mobile Subscriber Equipment (MSE) Network," *MILCOM '86*, pp. 39.4.1-39.4.7.
- 19 Fouad A. Tobagi, "Modeling and Performance Analysis of Multihop Packet Radio Networks," *Proceedings of the IEEE*, Vol. 75, No. 1, January 1987, pp. 135-155. See especially reference 15 from that paper.
- 20 J. L. Katz and B. D. Metcalf, "SURVNET: A Survivable Network Implementation," *IEEE JSAC*.
- 21 D. D. Clark, V. Jacobson, J. Romkey, and H. Salwen, "An Analysis of TCP Processing Overhead," *IEEE Communications Magazine*, Vol. 27, No. 6, June 1989, pp. 23-29.
- 22 Barry M. Leiner, Donald L. Nielson, and Fouad A. Tobagi, "Issues in Packet Radio Network Design," *Proceedings of the IEEE*, Vol. 75, No. 1, January 1987, pp. 6-20.
- 23 —, "Background to ATCCIS Communications," NATO ATCCIS Working Paper 34A.
- 24 U.S. Army AirLand Battle Plan (Heavy).
- 25 Meeting with MITRE Personnel in Bedford, Massachusetts, May 16, 1989.
- 26 Observed during meetings with MITRE Personnel in Bedford, Mass, and Air Force Personnel at Rome AFB, May 16-18, 1989.
- 27 —, 21st Century Tactical Command and Control Architecture, DARPA Order No. 3819, August 30, 1985.
- 28 —, "Navy Data Communications Program," video briefing by Naval Data Automation Command, OPNAVINST 2800.3.
- 29 —, "Voice and Data Integration in Tactical Networks," *MILCOM'88*.
- 30 —, "DMS Architecture."
- 31 —, "Background to ATCCIS Communications," NATO ATCCIS Working Paper 34A.
- 32 T. L. Mitchell, "A Super Network of the U.S. Air Force's Major Operational Commands," *MILCOM'88*, pp. 16.5.1-16.5.
- 33 —, "Background to ATCCIS Communications," NATO ATCCIS Working Paper 34A.
- 34 —, "DMS Architecture."